Escuela Universitaria de Ingeniería
Técnica de Telecomunicación
Universidad Politécnica de Madrid

PROYECTO FIN DE CARRERA

IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD PERIMETRAL

CARLOS MANUEL FABUEL DÍAZ

SEPTIEMBRE 2013

E.U.I.T. TELECOMUNICACIÓN

PROYECTO FIN DE CARRERA
PLAN 2000

TEMA: Seguridad de redes

TÍTULO: Implantación de un sistema de seguridad perimetral

AUTOR: Carlos Manuel Fabuel Díaz

TUTOR: Lourdes López Santidrián **Vº Bº.**

DEPARTAMENTO: DIATEL

Miembros del Tribunal Calificador:

PRESIDENTE: Juan Blanco Cotano

VOCAL: Lourdes López Santidrián

VOCAL SECRETARIO: Antonio DaSilva Fariña

DIRECTOR:

Fecha de lectura: 18 de Septiembre de 2013

Calificación: **El Secretario,**

RESUMEN DEL PROYECTO:

El presente proyecto está basado en un diseño y posterior implantación de un sistema de seguridad perimetral. Para ello, primero se han establecido las bases teóricas de los principales elementos de seguridad que conforman dichas implementaciones, y finalmente se ha desarrollado un entorno adecuado para unos requisitos establecidos.

Para la implantación de este proyecto se ha optado por los más importantes fabricantes de elementos de seguridad, eligiendo las soluciones de cada uno de ellos que mejor se adecuan a la infraestructura que se va a desplegar.

Además, una vez implementada la arquitectura, se realizarán una batería de casos de prueba para verificar el correcto funcionamiento de cada elemento.

También se diseña una metodología de gestión de incidencias, en la que se planifica las tareas a seguir cuando se produce cada una de las posibles incidencias que se puedan presentar, y se define una gestión de la propia plataforma, con un listado de tareas que asegura su óptimo funcionamiento.

1. RESUMEN

Este proyecto está desarrollado sobre la seguridad de redes, y más concretamente en la seguridad perimetral. Para mostrar esto se hará una definición teórico-práctica de un sistema de seguridad perimetral.

Para ello se ha desglosado el contenido en dos partes fundamentales, la primera incide en la base teórica relativa a la seguridad perimetral y los elementos más importantes que intervienen en ella, y la segunda parte, que es la implantación de un sistema de seguridad perimetral habitual en un entorno empresarial.

En la primera parte se exponen los elementos más importantes de la seguridad perimetral, incidiendo en elementos como pueden ser cortafuegos, IDS/IPS, antivirus, proxies, radius, gestores de ancho de banda, etc. Sobre cada uno de ellos se explica su funcionamiento y posible configuración.

La segunda parte y más extensa a la vez que práctica, comprende todo el diseño, implantación y gestión de un sistema de seguridad perimetral típico, es decir, el que sería de aplicación para la mayoría de las empresas actuales.

En esta segunda parte se encontrarán primeramente las necesidades del cliente y situación actual en lo que a seguridad se refiere, con los cuales se diseñará la arquitectura de red.

Para comenzar será necesario definir formalmente unos requisitos previos, para satisfacer estos requisitos se diseñará el mapa de red con los elementos específicos seleccionados. La elección de estos elementos se hará en base a un estudio de mercado para escoger las mejores soluciones de cada fabricante y que más se adecúen a los requisitos del cliente.

Una vez ejecutada la implementación, se diseñará un plan de pruebas, realizando las pruebas de casos de uso de los diferentes elementos de seguridad para asegurar su correcto funcionamiento.

El siguiente paso, una vez verificado que todos los elementos funcionan de forma correcta, será diseñar un plan de gestión de la plataforma, en el que se detallan las rutinas a seguir en cada elemento para conseguir que su funcionamiento sea óptimo y eficiente.

A continuación se diseña una metodología de gestión, en las que se indican los procedimientos de actuación frente a determinadas incidencias de seguridad, como pueden ser fallos en elementos de red, detección de vulnerabilidades, detección de ataques, cambios en políticas de seguridad, etc.

Finalmente se detallarán las conclusiones que se obtienen de la realización del presente proyecto.

2. ABSTRACT

This project is based on network security, specifically on security perimeter. To show this, a theoretical and practical definition of a perimeter security system will be done.

This content has been broken down into two main parts. The first part is about the theoretical basis on perimeter security and the most important elements that it involves, and the second part is the implementation of a common perimeter security system in a business environment.

The first part presents the most important elements of perimeter security, focusing on elements such as firewalls, IDS / IPS, antivirus, proxies, radius, bandwidth managers, etc... The operation and possible configuration of each one will be explained.

The second part is larger and more practical. It includes all the design, implementation and management of a typical perimeter security system which could be applied in most businesses nowadays.

The current status as far as security is concerned, and the customer needs will be found in this second part. With this information the network architecture will be designed.

In the first place, it would be necessary to define formally a prerequisite. To satisfy these requirements the network map will be designed with the specific elements selected. The selection of these elements will be based on a market research to choose the best solutions for each manufacturer and are most suited to customer requirements.

After running the implementation, a test plan will be designed by testing each one of the different uses of all the security elements to ensure the correct operation.

In the next phase, once the proper work of all the elements has been verified, a management plan platform will be designed. It will contain the details of the routines to follow in each item to make them work optimally and efficiently.

Then, a management methodology will be designed, which provides the procedures for action against certain security issues, such as network elements failures, exploit detection, attack detection, security policy changes, etc..

Finally, the conclusions obtained from the implementation of this project will be detailed.

3. INTRODUCCIÓN

3.1 Introducción

Cuando se habla de **seguridad perimetral**, nos estamos refiriendo a la forma de poner una barrera o frontera lo más inexpugnable posible entre nuestra red interna e Internet. El objetivo es restringir y controlar qué datos entran a nuestra organización o salen de ella. La principal ventaja de este tipo de seguridad es que permite al administrador concentrarse en los puntos de entrada, sin olvidar la securización del resto de servidores internos de nuestra red, para protegerlos frente a una posible intrusión.

Se puede caer en el error de pensar que podemos tener un sistema de seguridad total, descuidando el mantenimiento al no tener una política de seguridad implantada. En dicha política, algunos de los puntos más importantes serán el tener todos los equipos actualizados, realizar estudios de vulnerabilidades o una correcta planificación de backup.

3.2 Motivación del trabajo de fin de carrera

La motivación de este proyecto resulta de la problemática cada vez mayor de ataques e incidencias de seguridad en redes, ya sean a nivel local, a nivel empresarial, u otros tipos de escenarios.

Los elementos que se encuentran en dichas redes son susceptibles de diversos tipos de ataques, ya sea para la apropiación de datos, para la denegación del servicio que prestan, para la realización de estafas, etc.

Por ello, los sistemas encargados de protegernos de dichos ataques, cada vez están tomando más importancia y son más relevantes en el diseño de las organizaciones.
Este proyecto ofrece un sistema de seguridad perimetral típico, con el que no se garantiza una seguridad total, pero sí garantiza un importante nivel de seguridad a la empresa.

Con un sistema como el que se implanta, una correcta gestión de los elementos e incidencias, y una buena política de seguridad, la empresa estará libre de la mayor parte de las amenazas del exterior.

3.3 Entorno y contextualización

Zonas de seguridad y defensas perimetrales

La arquitectura de seguridad tiene como objetivo la defensa del **perímetro de red**. El perímetro es el punto o puntos de separación de la red interna confiable para la organización, que se encuentra en contacto con otras redes no fiables. Estas redes no fiables no sólo son la red de Internet, sino otras redes de usuarios o extranet relacionadas con la organización con los que se tenga conexión. El perímetro se delimita a través del uso de *líneas de cortafuegos* que actúan a modo de barrera separando de forma lógica las diferentes zonas de seguridad.

Las **zonas externas** engloban todos aquellos servicios y redes que realizan un uso intensivo de Internet y por tanto se caracterizan por un alto nivel de exposición frente a ataques o incidentes de seguridad al tener interconexión directa a la red pública de Internet. La **parte interna** engloba todos los sistemas internos, redes de usuarios internas y la interconexión con otras intranets y extranets relacionadas con la organización.

Ambas zonas deben ser salvaguardadas frente a la interconexión con otras redes ajenas a la organización o incluso diferentes segmentos lógicos cuyos niveles de seguridad no tienen por qué ser acordes con las Políticas de Seguridad de los activos que queremos salvaguardar.

Adicionalmente, se plantea una tercera zona de seguridad separada de las dos anteriores que engloba la parte de gestión de todos los activos informáticos y elementos de seguridad de la infraestructura. Esta zona de seguridad no es accesible desde fuera del perímetro de seguridad y a efectos del resto de redes es transparente.

Defensa en red

No obstante, de la defensa del perímetro, hay que proteger las redes internas frente a posibles ataques cuyo origen pueden ser las propias redes internas o intrusiones externas. Para ello, se introducen conceptos de segmentación de redes a nivel de infraestructura de red para evitar la visibilidad directa entre las mismas, el uso de sistemas de prevención de intrusiones para la monitorización y actuación frente a posibles ataques o comportamientos anómalos, e incluso la utilización de protocolos de cifrado IPSec/SSL para el trasporte seguro de los datos a través de redes no confiables como Internet y entre las propias redes internas identificadas.

Detección de intrusiones

Las redes más expuestas a ataques externos se encuentran monitorizadas a través de sistemas de prevención de intrusiones. Este tipo de sistemas se encargan de analizar todo el tráfico que pasa a través de la red en busca de patrones de posibles ataques. Su comportamiento puede ser simplemente informativo a través del envío de alertas o proactivo mediante la terminación de los distintos ataques detectados.

Arquitectura técnica

La arquitectura de red de un sistema de seguridad perimetral debe tener una estructura formada por dos capas de redes paralelas, aquellas que engloba todas las redes de producción, es decir, ofrecen servicios; y las redes de gestión que son utilizadas para la administración de los diferentes sistemas y elementos de seguridad. Ambas capas deben encontrarse plenamente redundadas y dimensionadas para alcanzar alta disponibilidad.

Las redes de producción deben estar divididas, tal como se ha comentado anteriormente, en dos grandes zonas: una parte externa y una parte interna. Ambas zonas deben encontrarse completamente aisladas y solamente unidas a través de un único punto controlado por el sistema de cortafuegos internos.

Ambas capas de red y zonas se encuentran segmentadas lógicamente en redes aisladas a través del concepto de redes locales virtuales VLAN. Se trata de un concepto de seguridad aplicable a nivel de redes de área local en las que un único dominio de difusión se divide a varios dominios disjuntos a través de la configuración de la electrónica de red. De esta forma aplicando la famosa regla del *divide y vencerás* se reduce el nivel de exposición frente ataques entre las redes, siendo éstas controladas por otros elementos de seguridad.

La zona externa estaría formada por subredes que corresponden a las redes DMZ (zona desmilitarizada) y la interconexión con la red pública de Internet, mientras que la zona interna estará formada por todas las redes internas.

El modelo de seguridad en una organización debería ser como muestra el siguiente gráfico, empezando por la seguridad perimetral y adentrándose poco a poco en la defensa de la red interna, siguiendo con la defensa de host, defensa de determinadas aplicaciones y finalizando con los datos.

Ilustración 1: Esquema de arquitectura de seguridad

Incidencias de seguridad y medición de riesgos

Se define como incidencia de seguridad a la circunstancia por la cual un determinado sistema experimenta una degradación parcial o total de su rendimiento, causando una degradación parcial o total del servicio prestado.

Se considera que las incidencias de seguridad se deben a tres razones principales:

- *Elección errónea* de las tecnologías empleadas en la arquitectura de seguridad (vulnerabilidades tecnológicas)

- *Mala configuración* de los dispositivos que constituyen la arquitectura de seguridad (vulnerabilidades de configuración)

- *Ausencia o definición deficiente* de las políticas de seguridad (vulnerabilidades asociadas a las políticas)

Puede darse el caso de que hayamos elegido la tecnología óptima para la protección de nuestra organización, pero si los productos que la implementan están mal configurados, habremos desaprovechado la inversión económica realizada.

Tal vez, hemos elegido la mejor tecnología y la hemos configurado según las políticas de la organización, pero si éstas no son las más adecuadas, seguiríamos siendo vulnerables.

Al contrario de lo que podríamos pensar a priori, un veinte por ciento de las incidencias se deben a vulnerabilidades técnicas (caracterizadas por la primera razón), mientras que un 80 por ciento de las incidencias se deben a vulnerabilidades organizativas (caracterizadas por las dos últimas razones), esto es, asociadas al uso que hacen los usuarios de las tecnologías de seguridad.

Las respuestas a preguntas como ¿la infraestructura de su red empresarial está protegida por uno o varios *firewalls*? ¿Hace uso de sistemas antivirus? Normalmente serían afirmativas. Sin embargo, las preguntas ¿existe un procedimiento para la elección y revisión de las contraseñas para el acceso a sus sistemas, especialmente los servidores más críticos? ¿Dispone de un procedimiento de backup de la información que éstos alojan? ¿Existe un procedimiento de revisión de logs para evitar posibles ataques o hacer un análisis del consumo de ancho de banda efectuado en la empresa? Y otras más que se podrían formular, tendría como respuesta un rotundo no.

Es precisamente esta situación la que hace al usuario el eslabón más débil de la cadena que constituye la arquitectura de seguridad, y en consecuencia, determina la seguridad de toda la arquitectura independientemente del estado de seguridad del resto de los componentes.

La seguridad ha dejado de ser un valor añadido a una red, para pasar a constituir a una característica indisoluble a ella. Hay que superar la concepción de que la seguridad se consigue con la adquisición de un cortafuego y empezar a entender que se trata de un proceso. Robert du Charme, director de Cisco Training Professional en Austin (Texas) afirma que: "No podemos gestionar aquello que no hemos medido, no podemos medir aquello que no hemos visto y no podemos ver aquello que no hemos buscado".

En efecto, el primer paso en el proceso de seguridad de una organización debería ser la "medición" de los riesgos que amenazan a la organización para así poder gestionarlos de forma eficiente. Para averiguar qué intentamos proteger y cuál es su nivel de riesgos aceptable, es preciso llevar a cabo lo que en la jerga técnica se denomina análisis de riesgos. El riesgo se estima como el impacto que se produciría si una determinada amenaza aprovecha una vulnerabilidad para poner en compromiso la seguridad de un recurso empresarial y la probabilidad de que esto ocurra. Si se representa la probabilidad de que tenga lugar un impacto frente a la magnitud del impacto, se puede apreciar que hay riesgos que no son de gran importancia porque aunque produzcan un gran impacto son extremadamente improbables o aunque ocurran muy a menudo, tendrían un impacto insignificante. Al resto de los riesgos, se les llama riesgos aplicables. Estos son los riesgos que se necesitan controlar.

Una vez que se ha llevado a cabo el "análisis de riesgos", conocemos su naturaleza y la prioridad que debe concederse a su gestión. Los cimientos sobre los que se sustenta la gestión de estos riesgos son las "políticas de seguridad" o documentos de seguridad. Éstas definirán los comportamientos aceptables, permitirán definir las herramientas y procedimientos necesarios, definirán una serie de responsabilidades e informarán cómo responder ante incidencias de seguridad, entre otras tareas, evitando así las vulnerabilidades asociadas a las políticas.

En este momento, nos encontramos en condiciones de poder definir un "plan de seguridad", a saber, una descripción detallada de los medios, herramientas o procedimientos para desarrollar las políticas de seguridad definidas anteriormente. Me permitirá averiguar el orden de implantación de las medidas en función de su prioridad y efectividad de la forma económicamente más rentable.

Como consecuencia de todo lo anterior, se llega a la conclusión de que hay que adoptar una serie de medidas que pueden consistir en el análisis exhaustivo a nivel técnico u organizacional de una determinada área de la organización ("auditoría de seguridad"). Como elemento complementario del análisis a nivel técnico, aunque también se puede desarrollar de forma independiente, resultan muy interesantes los "test de intrusiones". Éstos nos proporcionan información objetiva de cuán vulnerables somos frente a ataques perpetrados *hackers* o *crackers*.

Otras de las medidas, podría ser la "definición de arquitecturas de seguridad", analizando las tecnologías más apropiadas, los productos que las desarrollan de la forma económicamente más rentable y el diagrama de interconexión de todos ellos con la infraestructura presente. Podrá constar, pues, de un plan de migración y de unos procedimientos de explotación.

Posteriormente, será necesario instalar y configurar adecuadamente (evitando las vulnerabilidades de configuración) los productos seleccionados en la consultoría explicada en el párrafo anterior. Para estar seguros de que la configuración es segura procederíamos a realizar una "calificación de la arquitectura".

Por último, es preciso gestionar la arquitectura de seguridad para poder detectar la presencia de intrusos dentro de la red de la organización, reaccionar ante una incidencia, actuar proactivamente frente a posibles ataques mediante el "análisis de los logs" generados por el equipamiento de

seguridad, configurar remotamente determinados dispositivos, buscar la presencia de vulnerabilidades de orden técnico en los sistemas de la arquitectura y mantenerse actualizado sobre las nuevas amenazas que surgen en un área tan cambiante como la seguridad de la información.

3.4 Objetivos

El objetivo fundamental de este proyecto es dar a conocer a la gente, los conceptos más importantes en los que se basa la seguridad perimetral, realizando una demostración de lo que sería la implantación de un proyecto estándar en una organización ficticia.

El presente proyecto deberá proporcionar a dicha organización un entorno de seguridad que le garantice una integridad y protección de todos los activos que desee proteger, así como minimizar lo máximo posible todos los riesgos de interconexión a las redes externas.

Para poder mostrar muchos de los sistemas empleados en la seguridad informática, haremos que dicha organización necesite de entre otros los siguientes servicios:

- Tendrá la necesidad de publicar una Web en la que los clientes puedan interactuar y obtener información específica.

- Deberá tener un correo corporativo para la comunicación de los distintos empleados.

- Determinados trabajadores deberán poder conectarse a la red interna vía terminal móvil, PDA, u ordenador portátil mediante una conexión telefónica.

Se garantizará siempre un tráfico mínimo para determinadas aplicaciones, dando mayor importancia a las más críticas.

Para la realización del proyecto, se presentarán los sistemas de los que se valdrán para asegurar los servicios requeridos por dicha empresa, utilizando siempre los más empleados en el mundo de la seguridad de redes:

- Cortafuegos
- IDS e IPS (Sistemas de Detección de Intrusos)
- Antivirus de correo
- Proxys
- Frontales de correo
- Servidores de DNS
- Servidores radius
- Servidor de NTP
- Sistemas de gestión de ancho de banda
- Sistema de monitorización de equipos
- Sistemas de realización de backups

Para cada sistema o elemento de seguridad, se explicará su funcionamiento general, luego escogeremos una de las marcas más presentes en el mercado, y daremos algunas nociones de su correcta configuración.

Cumpliendo con los aspectos más importantes de todo sistema de seguridad, la arquitectura implantada deberá ser:

- Escalable: permitiendo siempre que se puedan añadir más elementos de seguridad u otros equipos a nuestra red.

- Tolerante a fallos: en la que después de un fallo se tarde el menor tiempo posible en la recuperación o pérdida de los menos datos posibles.

- Eficiente: que todos los sistemas de la arquitectura funcionen a su nivel óptimo, sin sobrecargarse pero sin infrautilizarse.

- Segura: lo más importante, que garantice el máximo posible de seguridad a nuestra red.

Una vez terminada la presentación del PFC, toda la gente que haya asistido podrá saber la configuración base de seguridad perimetral de la mayoría de las empresas que lo tengan implantado, así como tener unos conocimientos básicos de cada elemento de seguridad.

Se espera que este documento sirva de ayuda a dichas personas, para que en un futuro entiendan determinadas situaciones que puedan surgir en un entorno profesional de similares características.

1.5 Estructura de la memoria

La estructura de la memoria comprende 3 diferentes apartados:

1. Base teórica: En este apartado se detallaran los elementos más importantes presentes en cualquier infraestructura de seguridad perimetral.

2. Descripción experimental: está subdividido a su vez en 5 apartados:
    - Requisitos del cliente: En este punto se recogen las especificaciones técnicas mínimas que deben estar presentes en la infraestructura diseñada.
    - Implantación y adecuación de los elementos de seguridad en la empresa: Se detallan los mapas topológicos de la red, así como

los elementos de mercado que se utilizarán para conformar la estructura.

- Banco de pruebas: este punto comprende las pruebas que se realiza a cada elemento de seguridad para verificar su correcto funcionamiento.
- Gestión de la infraestructura: se detallan las pautas para la correcta gestión de cada elemento de seguridad.
- Metodología de gestión: especifica las distintas metodologías de gestión.

3. Conclusiones: se ofrecen las conclusiones a las que se llega después de realizar dicho proyecto.

4. BASE TEÓRICA: DESCRIPCIÓN DE ELEMENTOS Y SISTEMAS DE SEGURIDAD PERIMETRAL

Este tema se adentrará en los elementos base de cualquier infraestructura de seguridad perimetral, explicando en que consiste cada uno de ellos e indicando los diferentes funcionamientos que puedan existir en cada caso.

4.1 Cortafuegos

Un cortafuegos es un conjunto de componentes hardware y software destinado a establecer unos controles de seguridad en el punto o puntos de entrada a nuestra red, delimitando así la red interna (segura) y la red externa (insegura). La función básica de este sistema de seguridad es la de permitir o bloquear el tráfico entre dos redes en base a una serie de reglas. Su complejidad reside en las reglas que admiten y en como realizan la toma de decisiones en base a dichas reglas.

La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde fuera, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

Cuanto mayor es la red interna que protege un cortafuegos, mayor debe ser el esfuerzo de diseño para protegerla.

El nivel de protección que puede darnos un cortafuegos depende en gran medida de nuestras necesidades. Generalmente, los cortafuegos se configuran para protegernos contra cualquier intento de acceso desautorizado o no

correctamente autenticado desde el exterior hacia el interior de nuestra red, o viceversa.

No se debe olvidar nunca, que el cortafuegos es el punto de entrada a la red a proteger, pero hay amenazas contra las que un cortafuegos no puede hacer nada:

- Un cortafuegos no puede protegernos contra amenazas que no pasan a través de él. Como se decía anteriormente, el cortafuegos debe de ser el punto único e ineludible de acceso a la red interna. Si esto no es así su efectividad es sólo parcial.

- Tampoco puede proteger, generalmente, contra amenazas que proceden del interior de la red interna. Un empleado malicioso, un troyano o algunos tipos de virus pueden usar mecanismos válidos "desde dentro" para realizar acciones perniciosas.

- Igualmente, los cortafuegos no pueden proporcionar protección contra clientes o servicios que se admiten como válidos pero que son vulnerables ni contra virus.

- Los cortafuegos no pueden ni deben sustituir otros mecanismos de seguridad que reconozcan la naturaleza y efectos de los datos y aplicaciones que se estén manejando y actúen en consecuencia.

Además, lo frecuente es conectar al cortafuegos a una tercera red, llamada DMZ (zona desmilitarizada), en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

La DMZ es una red local que se ubica entre la red interna de una organización y la red externa, permitiéndose conexiones desde la red interna y la externa a

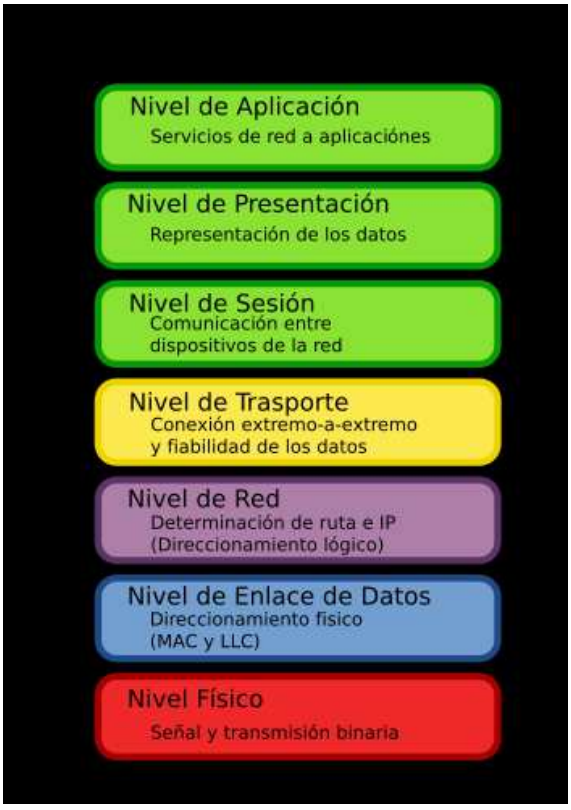
dicha red, mientras que desde la propia DMZ solo se podrán realizar conexiones hacia fuera. Normalmente esta red se utiliza para ubicar servidores que alojan servicios que deben estar accesibles desde fuera, como pueden ser los DNS, los servidores Web, los frontales de correo, etc.

La clasificación conceptual más simple divide los cortafuegos en sólo dos tipos:

- Cortafuegos a nivel de red (trabajan en las capas 2, 3 y/o 4).
- Cortafuegos a nivel de aplicación (trabajan en las capas 5,6 y/o 7).

Como regla general, podemos afirmar que cuanto más bajas sean las capas en las que el cortafuegos trabaja, su evaluación será más rápida y transparente pero su capacidad de acción ante ataques complejos es menor.

En el siguiente gráfico se puede observar la pila OSI para tener una mejor visión de lo mencionado arriba:



La industria, sin embargo, suele hacer una clasificación generacional más amplia:

- Las dos primeras generaciones están formadas por cortafuegos de red con una diferencia fundamental entre ellas: que tengan en cuenta o no información del estado de la conexión a la hora de evaluar las reglas.
- La tercera generación está orientada a filtrados a nivel de aplicación.
- Por último, la cuarta generación vuelve al nivel de red y está orientada al filtrado dinámico de paquetes.
- Incluimos un quinto apartado dedicado a los cortafuegos híbridos, última tendencia de la industria, los cuales pueden situarse simultáneamente en más de una de estas categorías.

Tenemos aún otra clasificación dependiendo del, por llamarlo de algún modo, "acabado externo" del producto. Así, tenemos cortafuegos que son meros servicios que se ejecutan sobre sistemas operativos robustos (como IPFilter o IPTables en el mundo Linux o CISCO Centri Firewall para tecnología NT), complejas herramientas modulares que pueden instalarse en varias máquinas (como es el caso de Firewall-1 de Check Point que posee dos módulos separados: inspección y gestión), o puede tratarse de sistemas dedicados que incluyen dentro de una caja compacta el hardware, el sistema operativo y el software específico, todo ello completamente listo para trabajar (es el caso del CISCO PIX Firewall).

A continuación se procederá a la explicación particular del funcionamiento interno de algunos de los cortafuegos arriba mencionados. Esta información la podemos ver en *[1]*:

- ***Filtrado de paquetes***

  Se trata del tipo más básico de cortafuegos. Analizan el tráfico de la red fundamentalmente en la capa 3, teniendo en cuenta a veces algunas características del tráfico generado en las capas 2 y/o 4 y algunas características físicas propias de la capa 1.

  Los elementos de decisión con que cuentan a la hora de decidir si un paquete es válido o no, son los siguientes:

  - La dirección de origen desde donde, supuestamente, viene el paquete (capa 3).
  - La dirección del host de destino del paquete (capa 3).
  - El protocolo específico que está siendo usado para la comunicación, frecuentemente Ethernet o IP aunque existen cortafuegos capas de desenvolverse con otros protocolos como IPX, NetBios, etc. (capas 2 y 3).
  - El tipo de tráfico: TCP, UDP o ICMP (capas 3 y 4).
  - Los puertos de origen y destino de la sesión (capa 4).
  - El interfaz físico del cortafuegos a través del que el paquete llega y por el que habría que darle salida (capa 1), en dispositivos con 3 o más interfaces de red.

  Con todas o algunas de esta características se forman dos listas de reglas: una de permitidas y otra de denegadas. La forma en que un paquete recibido se procesa en función de estas dos listas difiere según el modelo, el fabricante o el modo de actuación configurado y define en gran medida la permisividad del cortafuegos. Los más restrictivos exigen que el paquete pase con éxito por ambas listas, es decir, que no sea expresamente denegado en la una y sea expresamente autorizado en la segunda. Otras veces existe una única lista de reglas y el paquete es procesado según la primera regla que encontramos en la tabla y define

como tratarlo. Otros cortafuegos usan la última regla que encuentran como acción a efectuar. Por último, también encontramos diferencias en cuanto a qué hacer cuando no se encuentra ninguna regla válida: algunos productos aceptan el paquete y otros lo rechazan. Es, pues, fundamental conocer perfectamente el modo de trabajo del equipo que nos ocupa en cada momento.

Aparte de Aceptar (Accept) o Rechazar (Deny o Drop), la mayoría de los cortafuegos de este tipo poseen un tercer tipo de acción: Descartar (Discard). Cuando un paquete es procesado por una regla que define esta acción, este se elimina 'silenciosamente' sin devolverse error alguno al originario del mismo creando un efecto de 'agujero negro' y evitando así el cortafuegos revelar su presencia.

Las principales bondades de este tipo de cortafuegos están en su rapidez, transparencia y flexibilidad. Proporcionan un alto rendimiento y escalabilidad y muy bajo coste, y son muy útiles para bloquear la mayoría de los ataques de Denegación de Servicio, por ello se siguen implementando como servicios integrados en algunos routers y dispositivos hardware de balanceo de carga de gama media-alta.

Sus principales inconvenientes son su limitada funcionalidad y su dificultad a la hora de configurarlos y mantenerlos. Son fácilmente vulnerables mediante técnicas de spoofing y no pueden prevenir contra ataques que exploten vulnerabilidades específicas de determinadas aplicaciones, puesto que no examinan las capas altas del modelo OSI. La información almacenada en los logs de accesos es tan imprecisa como los parámetros usados en la configuración de su lista de reglas (direcciones de origen, de destino, puertos, protocolos, interfaces de red, etc.) y la complejidad en la construcción de reglas hace que deban de ser configurados por expertos conocedores del protocolo y que sean muy susceptibles a los errores.

No son, pues, efectivos como medida única de seguridad, pero si muy prácticos como primera barrera, en la que se bloquean ciertos ataques, se filtran protocolos no deseados y se pasan los paquetes restantes a otro cortafuegos que examine las capas más altas del protocolo.

- ***Inspección de estados***

Los cortafuegos de inspección de estado, o Stateful Inspection Firewall, son básicamente cortafuegos de filtrado de paquetes en los que, además, se valida a la hora de aceptar o rechazar un paquete el hecho de que este sea una petición de nueva conexión o pertenezca a un circuito virtual (o sesión) ya establecido entre un host externo y otro interno.

Cuando una aplicación crea una sesión TCP con un host remoto, se establece un puerto en el sistema 'originario' de la conexión con objeto de recibir allí los datos provenientes del sistema remoto. De acuerdo a las especificaciones de TCP, este puerto del host cliente estará comprendido entre el 1023 y el 16.384. En el sistema remoto se establecerá, asimismo, un puerto que será siempre menor al 1024.

Los cortafuegos por filtrado de paquetes deben de permitir tráfico entrante en todos los puertos superiores (1023 hasta 16.384) para permitir los datos de retorno de las conexiones salientes. Esto crea un gran riesgo de intrusiones. Los cortafuegos con inspección de estado resuelven eficazmente este problema construyendo una tabla con información correspondiente a todas las sesiones TCP abiertas y los puertos que utilizan para recibir los datos y no permitiendo el tráfico entrante a ningún paquete que no corresponda con ninguna de estas sesiones y puertos.

Para hacer esto, los cortafuegos de este tipo examinan rigurosamente el establecimiento de cada conexión (en la capa 4 del modelo OSI) para asegurarse de que esta es legítima y está permitida. Los paquetes no son remitidos a su destino hasta que el establecimiento de la conexión ha sido correctamente completado y verificado.

El cortafuegos mantiene una tabla de conexiones válidas (en la que se incluye información del estado de cada sesión) y deja pasar los paquetes que contienen información correspondiente a una entrada válida en dicha tabla de circuitos virtuales.

Una vez que la conexión finaliza la entrada en la tabla es eliminada y el circuito virtual entre los dos hosts es cerrado.

Las principales ventajas de este esquema de salvaguardas son la velocidad de filtrado, la solidez de sus principios de cara a establecer una política de seguridad y, en conjunto con un esquema de traslación de direcciones, la sólida protección adicional a las direcciones IP internas.

Sus principales debilidades residen en su limitación estrictamente al escrutinio del protocolo TCP, la imposibilidad de chequear protocolos de niveles altos, las limitaciones inherentes a su mecánica de actuación a la hora de llevar un registro de sucesos y la imposibilidad de implementar algunos servicios de valor añadido, como realizar cacheado de objetos http o filtrado de URLs (puesto que no 'entienden' estos protocolos).

Se suele utilizar este tipo de cortafuegos como primera línea de defensa inteligente (protege frente DoS) y que no consuma muchos recursos, dotando de una alta seguridad y escalabilidad al sistema.

- ***De aplicación***

  Los cortafuegos a nivel de aplicación constituyen sin duda un paso más en la evolución de los sistemas cortafuegos, ya que en este caso analizan todo el paquete a nivel de aplicación o, lo que es lo mismo, controlan no solo los puertos o las sesiones, sino el protocolo que se utiliza para la comunicación, evitando que puedan falsearse servicios. Por ejemplo, sería posible prohibir el acceso http independientemente de que el servicio http estuviera levantado en el puerto 80 o en el puerto 145, ya que el firewall analizará el protocolo de los paquetes y al ver http bloqueará la conexión.

  La proliferación de intrusiones a través de los aplicativos y la concienciación de las empresas por la necesidad de realizar auditorías de seguridad comenzaron a revelar que la mayor parte de los ataques que se sufrían venían derivados precisamente de fallos o vulnerabilidades en los aplicativos propios de las empresas. Estos aplicativos representaban, y hoy en día siguen representando, la mayor amenaza para las empresas.

  Contra estos problemas poco, o más bien nada, puede hacer un firewall (del nivel que sea), por lo que se hace necesario recurrir a nuevas soluciones que actúen como complemento a los sistemas de seguridad perimetral y que permitan de alguna manera paliar estos problemas que, en la mayor parte de los casos, se deben a deficiencias en la programación de las aplicaciones.

  Los firewall http son cortafuegos a nivel de aplicación que ofrecen protección para servidores Web, tratando de prevenir y controlar todos los posibles ataques y vulnerabilidades que se produzcan a nivel de

aplicación. Algunos pueden ofrecer además servicios de Proxy (ó Proxy inverso) de http.

Es decir, dentro de la evolución de los sistemas de firewall, los cortafuegos http se centran en la protección de las aplicaciones situadas en servidores Web y, por tanto, deben ocuparse de todo lo asociado con el protocolo http.

Se pueden definir dos estrategias generales distintas a la hora de implementar estos firewall:

1. La primera estrategia se basa en dos aproximaciones complementarias:

   Por un lado, se implementan reglas de filtrado basadas en añadir ataques conocidos a servidores Web. Esta información de ataques (firma) puede ser obtenida tanto de herramientas de prueba de vulnerabilidades, que simulan ataques a servidores Web, como de la información de vulnerabilidades conocidas asociadas a estos servicios Web.

   En segundo lugar, el mecanismo de filtrado se basa en el tráfico http habitual del servicio actualmente desplegado. El análisis de este tráfico permite definir una serie de generalidades asociadas al servicio (URLs y métodos permitidos, contenido en la llamada de aplicaciones, etc.) que permiten implementar una política "todo lo que no está expresamente permitido está prohibido"; que puede denegar, de forma directa, los ataques ya sean conocidos o no. Sin embargo, hay que recalcar que esto puede ser difícil de definir para ciertos ámbitos y entornos.

2. La segunda estrategia consiste en implementar el protocolo HTTP tal y como está definido en los estándares de Internet, prohibiendo a cualquiera que trate de romper la seguridad de las aplicaciones protegidas usando peticiones deformadas o modificando peticiones legítimas.

Ambas estrategias son compatibles y/o complementarias entre sí. Son muchos los ataques que pueden bloquear estos sistemas, a continuación se citan los más importantes y relevantes de ellos:

- Filtrado de URLs: Un grupo de ataques habituales a servidores Web, realizados por herramientas automáticas y gusanos, se realizan a través de URLs que aprovechan vulnerabilidades específicas de los servidores web. Por tanto deben ser capaces de filtrar URLs, tanto definidas de forma completa, como a través de expresiones regulares. Esta información se recoge en firmas y las solicitudes web que incorporen estas firmas deben ser bloqueadas por el firewall.

- Control de protocolo http: Ofrecen una alta granularidad en el control de la funcionalidad ofrecida en el protocolo http. Así, se pueden controlar tanto las operaciones (GET, POST, PUT, DELETE, TRACE...) como los parámetros que se incluyan en dichas operaciones. Se exige conformidad completa con el protocolo, y se pueden filtrar solicitudes de un tipo concreto (User-Agent de sólo unos tipos concretos,...).

- Resistencia y mitigación a ataques de denegación de servicio

- Ataques a aplicaciones vulnerables: La mayoría de servidores Web, al ser instalados por defecto, incluyen páginas de ejemplo y aplicaciones que pretenden mostrar las capacidades del servidor a los nuevos usuarios; suelen ser vulnerables a ataques y por tanto activamente explotadas por crackers. Estos firewalls detienen el acceso a estas páginas que no están directamente referenciadas en el sitio web.

- Problemas de implementación de servidor: Se trata de eliminar los problemas generados por los errores en la implementación de los servidores Web, como el error de programación en Unicode encontrado en IIS, o el desborda-miento de memoria shtml en Iplanet.

- Manipulación de campos ocultos: Existen unos campos de formularios no visualizables por el usuario final, donde las aplicaciones almacenan la información de sesión. Se puede acceder a ellos a través del código fuente de la página HTML o de la barra de direcciones del navegador, y por tanto son susceptibles de ser modificados por cualquier atacante. Lo que se hace es proteger los campos con firmas digitales para que no sean modificados, o bloquear los ataques y registrarlos.

- Desbordamiento de memoria (buffer overflow): Solucionan los problemas de desbordamiento de memoria, que presentan las aplicaciones que confían en los límites de la longitud del campo de los formularios, ya que esta limitación es fácilmente superable.

- Deterioro de cookies: A través de, por ejemplo, la firma digital del contenido, se evitan los problemas de seguridad generados por la información transitoria almacenada en las cookies.

- Cross-site scripting: Este problema es cada vez más frecuente, y consiste en hacer creer a una persona que está accediendo a un sitio web cuando en realidad lo está haciendo al otro, con el fin de conseguir información como el login del usuario, o los datos de su tarjeta de crédito.

- Puertas traseras: Este tipo de ataque consiste en que a través de parámetros específicos a la hora de acceder a una aplicación, se puede llegar a una puerta trasera en el servidor, o alcanzar una función de depuración que visualiza información prohibida, lo cual permitiría a un cliente remoto entrar en el servidor.

Existen diversas formas de realizar la implantación de este tipo de cortafuegos, y la elección de una solución u otra dependerá de las funcionalidades que ofrezca el producto escogido y de la configuración de la red del cliente.

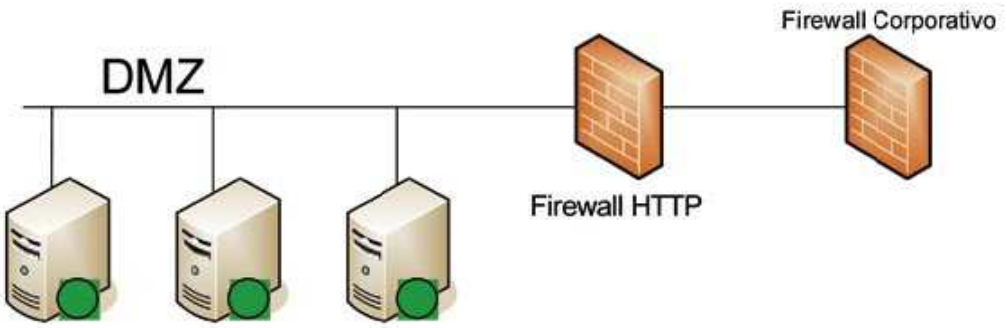
En primer lugar y como ya se ha mencionado anteriormente, estas soluciones no sustituyen en ningún caso a los firewalls tradicionales, sino que suponen un complemento a la seguridad que estos ofrecen. Por lo tanto en todas las soluciones mostradas a continuación aparecerán tanto los firewalls corporativos, como los firewalls http.

Una de las soluciones habituales para el despliegue de este tipo de cortafuegos consiste en su instalación en modo bridge

transparente situado en la DMZ, donde se ubican los servidores web, de forma que todo el tráfico pase por este equipo antes de llegar a los servidores finales.

De esta forma, el firewall http puede analizar el tráfico destinado a los servidores, aplicando la política establecida sin interferir ni en la configuración de los firewalls corporativos ni en la de los servidores web.

El principal inconveniente de este tipo de implantaciones radica en que todo el tráfico destinado a los servidores web, ya sea http, ftp, smtp o cualquier otro tráfico permitido por la política de los firewalls corporativos, atravesará el firewall http aunque no tenga nada que hacer con dicho tráfico. Por el contrario la ventaja fundamental es la sencillez de instalación, puesto que no interfiere con la arquitectura actual y no se precisan cambios en la misma.



Otra opción a la hora de implantar estas soluciones consiste en la definición del firewall http como un servicio "Proxy inverso", que responde a las peticiones que llegan desde Internet como si se

tratase de los propios servidores web y luego encamina esas peticiones a los servidores destino, filtrando todo aquel contenido que pudiera vulnerar la política establecida en el firewall o suponer un peligro para los servidores web.

- ***Híbridos***

Se trata de cortafuegos que utilizan varias de las tecnologías enumeradas anteriormente, para así poder unir las mejores características de cada una de las plataformas.

Así, por ejemplo, podemos encontrar con facilidad cortafuegos a nivel de aplicación con servicios de proxy que incluyen filtrado de paquetes para inspeccionar las tramas UDP que antes le estaban restringidas.

En definitiva, la hibridación de tecnologías y la amalgama de características de los actuales productos ha potenciado las ventajas de estos equipos pero también ha complicado en gran medida la tarea de elegir cuál es el cortafuegos más adecuado a nuestras necesidades.

Este tipo de cortafuegos interceptan los paquetes entre las capas 2 y 3 del modelo OSI, extrae aquí la información relativa al estado de la conexión y mantiene dinámicamente unas tablas con información sobre el estado de las conexiones abiertas o en trámites de ser establecidas.

El módulo de inspección se encarga de ir inspeccionando todos los paquetes entrantes y salientes que pasan por las interfaces de red. Ningún paquete es procesado por las capas superiores hasta que el motor de inspección verifica que cumple con las políticas de seguridad establecidas.

Un valor añadido sobre los cortafuegos actuales son los servicios adicionales de que disponen y que facilitan las labores de protección y administración de la red. Se trata de servicios en algunos casos hechos a medida y en otros habituales de otros dispositivos pero que, en cualquier caso, representan un punto importante a la hora de decidirnos por una u otra implementación.

A continuación se detallan algunos de estos servicios mencionados:

- ***Translación de Direcciones de Red (NAT)***

Los servicios de NAT (Network Address Translation) resuelven dos de los principales problemas de seguridad e infraestructura de las redes actuales. En primer lugar, constituyen una herramienta muy efectiva para esconder las direcciones de red reales de nuestra red interna. En segundo lugar, y debido a la reducción del espacio de direcciones IP disponibles, muchas organizaciones usan NAT para permitir la salida a Internet de sus equipos de la red interna con un mínimo de direcciones legalmente válidas.

- ***Protocolo de Configuración Dinámica de Hosts (DHCP)***

DHCP, Dynamic Host Configuration Protocol, es un servicio de asignación automática de direcciones IP con importantes y evidentes ventajas administrativas a la hora de mantener redes de tamaño medio / amplio que muchos Cortafuegos (sobre todo los que trabajan en las capas 2, 3 y/o 4) incluyen como valor añadido.

- ***Redes Privadas Virtuales (VPN)***

  Uno de los servicios adicionales más valorados de los Cortafuegos actúales es la posibilidad de construcción de Redes privadas Virtuales (VPN o Virtual Private Networks) que permiten extender a las comunicaciones externas la seguridad del interior de nuestra red.

  Una VPN se construye en la cúspide de la pila de protocolos ya existentes en la red usando protocolos adicionales y fuertes cifrados y mecanismos de control de integridad, sustitución o repetición de la información transmitida.

  Existen diferentes formas de construir una VPN. Quizás la forma más lógica y comúnmente usada es utilizar para ello el estándar IPSec., consistente en una porción de las características de seguridad de IPv6 separadas y portadas para ser usadas en IPv4.

  Otras opciones son el estándar de Microsoft llamado PPTP (Point to Point Tunneling Protocol) o L2TP (Layer 2 Tunneling Protocol), propuesto por la IETF (Internet Engineering Task Force).

- ***Alta Disponibilidad y Balanceo de Carga***

  Como hemos visto en las descripciones anteriores, uno de los principales inconvenientes de los cortafuegos es la disminución del rendimiento que provocan, efecto que se ve agravado en algunos esquemas más que en otros.

  Los cortafuegos empresariales de gama alta suelen ofrecer una solución para paliar este problema al mismo tiempo que ofrecen redundancia mediante el balanceo de carga entre dos o más dispositivos cortafuegos.

Logramos, de esta forma, mejorar el problema del rendimiento y ofrecer alta disponibilidad y tolerancia a fallos en nuestra política de seguridad.

- ***Integración con Sistemas de Detección de Intrusos (IDS)***

  Los sistemas de detección de Intrusos son herramientas o dispositivos que nos permiten inspeccionar nuestro sistema y generar alertas que nos permitan conocer cuando alguien ha tratado de penetrar en nuestro sistema o lo ha conseguido.

  Se trata de una tecnología relativamente nueva y en un grado aún bajo de madurez, pero que va ganando cada vez más importancia y mejores resultados.

  Existen dos tipos de sistemas IDS los de hosts y los de redes. Los de redes se subdividen, a su vez, en distribuidos o no. Los IDS de hosts se basan en el análisis de las estadísticas de uso o el uso indebido de ciertos recursos comandos, archivos, etc.) del sistema. Los IDS de red buscan patrones sospechosos en los paquetes TCP, malformaciones en la estructura de los mismos, etc. Se trata, pues, de sniffers que poseen tablas (actualizables) con los patrones característicos usados en los intentos de entrar en un sistema.

4.2 IDS e IPS (Sistemas de Detección de Intrusos)

Conocidos como mecanismos de detección o prevención de intrusiones, los IDS/IPS se han convertido en una obligación de dispositivos que han de tener las organizaciones como mecanismos de seguridad en su infraestructura.

Dependerá del uso que se les vaya dando a estos dispositivos, que se conviertan en herramientas útiles que aporten valor en el proceso de la

seguridad de las organizaciones, o se conviertan en unos "cacharros" más, cuyo mantenimiento engrose la lista de tareas de los administradores. Ya que todos los dispositivos que forman parte del staff de una compañía requieren un mantenimiento (backups, actualizaciones, parches, licencias,...) por lo menos se darán las pautas para que la utilización de sondas de detección/prevención de intrusiones puedan resultar útiles en su funcionalidad.

Antes que nada, hay que dejar claro que las sondas IDS son dispositivos que se posicionan offline del flujo de las redes, de manera que reciben una copia del tráfico de cada VLAN (mediante la utilización de TAPs físicos o con la creación de un port mirroring o port span de una VLAN de un switch capaz de hacerlo), siendo ésta una gran ventaja ya que no retardan el flujo del tráfico de producción. Por un interfaz sin pila TCP/IP reciben el tráfico en formato RAW y lo analizan enfrentándolo contra una base de datos de firmas de ataques conocidos, de manera que, a través de otro interfaz, cuando detectan tráfico malicioso, envían señales de alarmas a una base de datos centralizada. La desventaja es que no pueden detener ataques de un único paquete y necesitan de otros dispositivos de red (routers, firewall) para detener un ataque.

Estos dispositivos solamente son capaces de detectar tráfico y, en ciertas ocasiones, pueden llevar a cabo reacciones activas que eviten males mayores en la infraestructura de producción. En este caso se hace referencia a IDS de red, puesto que existen los llamados IDS de host.

Los IDS de host o sondas de host son agentes software que se instalan de forma directa en cada uno de los servidores a monitorizar y que enviaban alertas sobre ataques contra los mismos.

Tal y como se indica en *[2]*, un IDS de host analiza diferentes áreas para determinar el uso incorrecto (actividades maliciosas o abusivas dentro de la red) o alguna intrusión (violaciones desde fuera). Estos IDS consultan

diferentes tipos de registros de archivos (kernel, sistema, servidores, red, cortafuegos, y más) y comparan los registros contra una base de datos interna de peculiaridades comunes sobre ataques conocidos.

Los IDS instalados en Linux y Unix hacen uso extensivo de syslog y de su habilidad para separar los eventos registrados por severidad (por ejemplo, mensajes menores de impresión versus advertencias importantes del kernel). El comando syslog está disponible cuando se instala el paquete sysklogd, incluido con Red Hat Enterprise Linux. Este paquete proporciona el registro de mensajes del sistema y del kernel.

Los IDS de host filtran los registros (lo cual, en el caso de algunas redes y registros de eventos del kernel pueden ser bastante detallados), los analizan, vuelven a etiquetar los mensajes anómalos con su propia clasificación de severidad y los reúne en su propio registro para que sean analizados por el administrador.

Los IDS basados en host también pueden verificar la integridad de los datos de archivos y ejecutables importantes. Funcionan verificando una base de datos de archivos confidenciales (y cualquier archivo añadido por el administrador) y crea una suma de verificación de cada archivo con una utilidad de resumen de archivos de mensajes tal como md5sum (algoritmo de 128-bit) o sha1sum (algoritmo de 160-bit). El IDS luego almacena las sumas en un archivo de texto plano y periódicamente compara las sumas de verificación contra los valores en el archivo de texto. Si cualquiera de estas sumas no coinciden, el IDS alertará al administrador a través de un correo electrónico u otro tipo de alerta.

Los IDS de host pueden combinar las mejores características de antivirus, cortafuegos de red y cortafuegos de host, mejorando su seguridad utilizando reglas que controlan el sistema operativo y la pila de red.

Según se indica en *[3]*, los IPS sin embargo, funcionan de una forma diferente, puesto que se emplazan en modo inline entre las diferentes redes, de modo que el tráfico que pasa hacia y desde una red los ha de atravesar, pudiendo discriminar si el tráfico es malicioso o no.

Al encontrarse en modo transparente e inline, este tipo de dispositivo sí que es capaz de bloquear todo tipo de tráfico que se considere un ataque. En líneas generales, el funcionamiento principal de los IPS a la hora de identificar ataques es idéntico al de los IDS. Se basan en firmas de ataques conocidos y envían por un tercer interfaz las alertas a una base de datos centralizada.

Como diferencias principales entre ambos, aparte de las ya comentadas referidas a la capacidad de detectar únicamente o de bloquear los ataques, es la cantidad de tráfico a monitorizar por parte de ambos. En el caso de los IPS, sólo son capaces de identificar ataques dentro del tráfico que los atraviesa en ambos sentidos. Sin embargo, los IDS de red van más allá, puesto que al analizar el tráfico de una VLAN completa, es capaz de clasificar ataques entre máquinas de la VLAN, no sólo la que pasa de una red a otra.

Algunas de las acciones que puede realizar un IPS cuando detecta una anomalía son las siguientes:

- *Denegar al atacante*: denegar el paquete actual y los futuros desde la dirección IP del atacante durante un tiempo.
- *Denegar la conexión:* denegar el paquete actual y los futuros de una conexión TCP.
- *Denegar un paquete*.
- *Registrar los paquetes de un atacante*: registrar los paquetes que provienen de la dirección IP del atacante.
- *Registrar los paquetes de ambos*: registrar los paquetes del atacante y de la víctima.
- *Registra los paquetes de la víctima*.

- *Producir una alerta*.
- *Producir una alerta detallada*: añade un volcado codificado del paquete malicioso.
- *Solicitar el bloqueo de la conexión*: enviar a un dispositivo el bloqueo de una conexión.
- *Solicitar el bloqueo del equipo*: enviar a un dispositivo el bloqueo de la IP del atacante.
- *Enviar un SNMP trap*.
- *Resetear la conexión TCP*: interceptar la conexión TCP y terminarla en los dos extremos.

Como se vio anteriormente, los IDS e IPS, controlan los posibles ataques mediante firmas. Una firma de red es un conjunto de reglas utilizadas para detectar actividades intrusivas. Los sensores examinan los paquetes de red utilizando las firmas para detectar ataques conocidos.

Los tipos de alertas asociadas a dichas firmas son los siguientes:

- *Falso positivo*: tráfico legítimo genera una alarma.
- *Falso negativo*: no se detecta el ataque.
- *Verdadero positivo*: se detecta el ataque.
- *Verdadero negativo*: el tráfico legítimo no genera una alarma.

Para finalizar, se exponen algunas ventajas y desventajas de los IDS/IPS:

Ventajas de los IDS

- No añaden latencia
- Un fallo del sensor no paraliza la red

Desventajas de los IDS

- No detienen todos los paquetes maliciosos

- Son más vulnerables a técnicas de evasión

Ventajas de los IPS

- Detienen todos los paquetes maliciosos
- Pueden normalizar el flujo de tráfico y eliminar las técnicas de evasión

Desventajas de los IPS

- Añaden latencia
- Un fallo en el sensor paraliza la red

4.3 Antivirus de correo

Tal y como se indica en *[4]*, se conoce a un servidor SMTP como un servicio instalado en un equipo que es capaz de procesar y enviar correo electrónico, así como de recibirlo y distribuirlo según esté configurado. En una empresa que maneja internamente su correo electrónico, muchas veces el servidor SMTP es por donde le llega el correo electrónico a su red, y por ello, la primera línea de defensa contra virus que se distribuyan de esta manera.

Los servidores SMTP pueden estar integrados en un servidor de mensajería, o trabajar en forma separada como muchas veces sucede en aquellos instalados bajo Linux. Cuando trabajan individualmente, también se conocen como MTA (Mail Transport Agent) y suelen trabajar en forma asociada con un MDA (Mail Delivery Agent).

Por lo tanto, la función será recibir el correo entrante procedente de servidores externos (no confiables), analizar en busca de virus, y si el resultado es satisfactorio mandarlos al servidor de correo interno, que será el encargado de distribuir los correos a cada cliente. En el caso de los correos salientes, será el servidor de correo interno el que mande los mails al antivirus, éste los analizará, y si están libres se mandarán al servidor externo.

Una solución antivirus para servidores SMTP debe ser capaz de identificar, desinfectar y rechazar mensajes de correo electrónico infectados y notificar al administrador. Es un factor importante que cuente con algún tipo de protección heurística, dado que el detectar amenazas desconocidas es muy importante a este nivel, y que pueda trabajar independientemente de la solución instalada en el servidor para manejar el correo electrónico, si es necesario.

Los servidores de mensajería, de los cuales los más conocidos son Microsoft Exchange y Lotus, entre otros, son aquellos cuya función principal es encargarse de almacenar y distribuir el correo electrónico entre sus clientes. Muchas veces incluyen otras herramientas, como un servidor SMTP integrado, aplicaciones de colaboración, etc.

Si no se cuenta con un antivirus a nivel de servidor SMTP, o si simplemente éste no fue capaz de detectar un virus, el mensaje infectado terminará almacenado en el servidor de mensajería hasta que el usuario lo descargue. Para evitar este tipo de problemas, es importante contar con un buen antivirus capaz de detectar mensajes infectados cuando son procesados por el servidor de mensajería (antivirus instalado a parte del propio de smtp), además de ser capaces de explorar por virus los mensajes almacenados en el servidor.

Tanto en los servidores de SMTP como de mensajería, será un factor interesante que la solución antivirus cuente con la posibilidad de configurar reglas de filtrado que permitirá mantener una protección más eficiente contra los virus que aprovechan el correo electrónico, como los gusanos.

Para el tratamiento de los correos, es fundamental que los antivirus estén siempre actualizados, programando actualizaciones manuales o automáticas diariamente. En dichos antivirus, hay multitud de filtros, ya sean por virus, o por spam. Todo antivirus debe tener una lista de firmas de anti-spam, extensiones de ficheros adjuntos, listas de servidores que se encuentren en

listas negras, palabras claves encontradas en la cabecera del correo o en el cuerpo, etc.

4.4 Proxy Cache Web

Como se puede ver en *[5]*, se trata de sistemas de seguridad que permiten a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página web) en una cache que permita acelerar sucesivas consultas coincidentes.

Aparte de la utilidad general de un proxy, proporciona una cache para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

El funcionamiento de un proxy cache web es siguiente:

1. El cliente realiza una petición (p.e. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.

2. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, devuelve el documento inmediatamente, si no es así, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda una copia en su caché para futuras peticiones.

La caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de ella, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

Dicho filtrado de webs, se hace mediante listas de URLs prohibidas, que pueden estar clasificadas según al tipo que pertenezcan, como son el juego, redes sociales (como pueden ser facebook o tuenti) entretenimiento, pornografía, etc. De esta manera, una organización puede restringir el acceso a determinadas web que considere que puede ser perjudicial para el buen funcionamiento, o incluso para la distracción y el mal aprovechamiento del tiempo de trabajo.

Ventajas

- *Ahorro de Tráfico*: Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.

- *Velocidad en Tiempo de respuesta*: El servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante

un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.

- *Demanda a Usuarios*: Puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.

- *Filtrado de contenidos*: El servidor proxy puede hacer un filtrado de páginas o contenidos basándose en criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.

- *Modificación de contenidos*: Basándose en la misma función del filtrado, y llamado Privoxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Desventajas

- Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché. Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.

- El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.

- Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

4.5 Antivirus de navegación

Se debe empezar antes de nada a pensar en si se puede o no llevar a cabo una navegación segura sin la utilización de un antivirus de navegación.

Tal y como se indica en *[6]*, la teoría de la navegación segura no es que sea excesivamente fiable, ya que la vía de entrada de un virus al ordenador es muy variada (descargas, visitas a páginas, correo, chat, intercambio de archivos, reenvíos de mensajes de correo...), y alguna de ellas son bastante difíciles de controlar por el usuario. Además, ¿qué es exactamente lo que se entiende por una navegación segura? ¿Movernos solo por páginas con seguridad activada (HTTPS)? El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado, pero es tan solo eso, una seguridad en cuanto al tráfico, no en cuanto a que contenga algún tipo de malware o no. ¿Visitar tan solo páginas oficiales o conocidas? Si en esto es en lo que nos basamos más vale que tengamos mucho cuidado, porque en cualquier momento podemos entrar en una página que no lo sea tanto.

Además, este tipo de navegación nos va a defender tan solo de un porcentaje relativamente pequeño de probabilidades de infección, pero si utilizamos el correo electrónico, programas de mensajería instantánea (y, sobre todo, hacemos algún intercambio de archivos, por pequeños que sean y del tipo que sean, a través de ellos) o tenemos algún tipo de programa de descargas o intercambio, de poco nos sirve el que seamos sumamente cuidadosos en nuestra navegación si luego no tenemos un programa que nos avise de la existencia de un virus en cualquier archivo que nos hayan podido enviar.

Y todo esto es aplicable de igual forma a los navegadores. Tampoco es cierto que existan navegadores seguros al 100%. Evidentemente un navegador expuesto a miles de ataques es más fácil que sea más vulnerable que otro no tan expuesto, pero, al igual que pasa con los sistemas operativos, esto no constituye una seguridad en sí, ya que por un lado esta circunstancia puede

cambiar, y por otro el que tenga menos no quiere decir que no los tenga ni que los que pudiera tener no sean efectivos. Fallos de seguridad pueden tener (y de hecho tienen, como demuestran estudios realizados por empresas independientes dedicadas a la seguridad informática) todos los navegadores, y la idea de intentar cubrirlos todos es tan utópica como la de crear una vacuna contra todas las enfermedades, incluso contra las que no se han descubierto aún.

Por otro lado, la inversión en seguridad puede ser casi nula, ya que hay en el mercado tanto antivirus como anti espías y anti malware gratuitos que funcionan muy bien, y aun en el supuesto de que su rendimiento sea bajo o inferior al de versiones de pago (que en muchos casos suele ser cierto), más vale la protección que nos ofrecen (aunque, repito, no sea muy grande) que no tener ninguna.

Hay que tener en cuenta otra cosa fundamental, y es que los programas anti malware (antivirus y demás) nos van a proteger de la mayoría de los ataques, pero no son un seguro al 100%, y no nos garantizan que no vamos a terminar infectados. Esta seguridad no la podemos tener por una razón muy simple, y es que son miles las mutaciones sobre virus existentes las que salen a diario (en realidad virus nuevos salen muy pocos), y si bien existen técnicas de detección heurística que resultan muy eficaces, muy eficaz no significa infranqueable.

Ahora ya, sabiendo que es fundamental la utilización de un antivirus de navegación se pasará a explicar el funcionamiento genérico de dichos dispositivos.

Los antivirus de navegación siempre trabajan junto con los ya mencionados Proxy/caché, de tal manera que éstos almacenen las páginas donde los usuarios ya han navegado, y así evitar que se tenga que descargar de nuevo.

Los usuarios deberán poner la dirección del Proxy en su navegador web, si el Proxy tiene la web en su caché, directamente se la mostrará al usuario, y si no la tuviera hace la petición al antivirus, que será el encargado de realizar la petición a la dirección web.

Una vez que esté descargando dicha web, es cuando efectuará el análisis del contenido, pudiendo no devolver la web si contiene mal ware, eliminando algún elemento de dicha web, o devolviendo la totalidad de la web sin modificar al Proxy, que será el que finalmente la muestre al usuario.

El análisis que lleva a cabo un antivirus se puede realizar de distintas maneras y en combinación de todas ellas, en las que algunas son:

- Bloqueo de determinados servidores, de los que normalmente se sabe que pueden tener mal ware, o simplemente que se desconfía de ellos.
- Bloqueo de determinados tipos de ActiveX, scripts, documentos embebidos en otros, etc.
- Bloqueo de determinados archivos con extensiones de ejecutables, como puedan ser exe, dll, sys…
- Firmas en los que se recogen los principales tipos de exploits, por lo que el antivirus irá comparando lo descargado con estas firmas.
- Bloqueo de páginas en las que se encuentre un determinado número de palabras prohibidas, con lo que si se repiten mucho se podrá saber que esa página no es una web "lícita" o segura, y se bloqueará.

Adicionalmente también se podrán añadir servidores web que no se quiera que el antivirus realice el escaneo por considerarlos seguros, con el consiguiente riesgo que esto puede acarrear.

Para finalizar, y con todo lo anteriormente expuesto, se puede decir que es de vital importancia que un antivirus esté perfectamente actualizado. La pérdida de tan solo unos días de actualizaciones puede hacer que nuestro antivirus sea

totalmente ineficaz ante cientos de virus, o ante la alteración de cualquiera de ellos, haciendo que las firmas no valgan de nada.

4.6 Servidores de DNS

Tal y como comenta *[5]*, un servidor DNS (Domain Name System) se utiliza para proveer a las computadoras de los usuarios (clientes) un nombre equivalente a las direcciones IP. El uso de este servidor es transparente para los usuarios cuando éste está bien configurado.

El DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Esta base de datos jerárquica, es al estilo de cómo son los sistemas de ficheros de UNIX. La raíz de la base de datos está representada por el nodo "." y cada uno de los nodos que descienden de ella reciben el nombre de dominios. En el sistema DNS cada dominio se hace cargo de la base de datos que depende de él.

Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

En cada dominio puede haber a su vez servidores y otros dominios. Cada nombre de dominio se construye escribiendo los sucesivos nombres de dominio a los que pertenece el dominio hasta llegar al dominio raíz. Cada nombre se separa del siguiente mediante un punto y se escriben colocando a la izquierda los nodos inferiores. Por ejemplo el departamento imasd de la compañía acme, que operase en España recibiría el nombre: imasd.acme.es

El punto raíz no se pone. A un nombre de dominio que incluye todos los nodos hasta el raíz se le denomina nombre de dominio completamente cualificado

(FQDN Full Qualified Domain Name). En Internet por debajo del raíz los primeros nodos corresponden normalmente a países u organizaciones internacionales. Cada país tiene su propio dominio, y además existen otros para otro tipo de organizaciones.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

Cada LAN (Red de área local) debería contar con un servidor DNS. Estos servidores trabajan de forma jerárquica para intercambiar información y obtener las direcciones IP de otras LANs.

Componentes del DNS

- Los Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde a nombre.dominio?);

- Los Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada.

- Y las Zonas de autoridad, porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

Tipos de resolución de nombres

Existen dos tipos de consultas que un cliente puede hacer a un servidor DNS:

- Recursiva
- Iterativa

En las consultas recursivas, consisten en la mejor respuesta que el servidor de nombres pueda dar. El servidor de nombres consulta sus datos locales (incluyendo su caché) buscando los datos solicitados.

Las consultas iterativas, o resolución iterativa el servidor no tiene la información en sus datos locales, por lo que busca un servidor raíz y repite el mismo proceso básico (consultar a un servidor remoto y seguir a la siguiente referencia) hasta que obtiene la respuesta a la pregunta.

Cuando existe más de un servidor autoritario para una zona, Bind utiliza el menor valor en la métrica RTT (round-trip time) para seleccionar el servidor. El RTT es una medida para determinar cuánto tarda un servidor en responder una consulta.

El proceso de resolución normal se da de la siguiente manera:

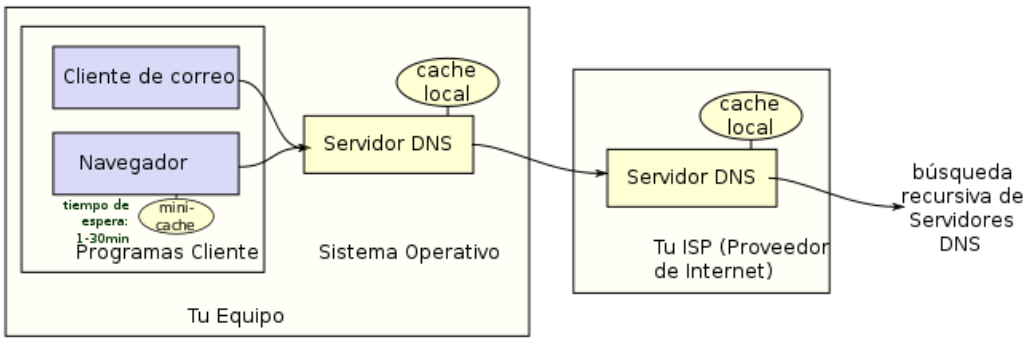
- El servidor A recibe una consulta recursiva desde el cliente DNS.
- El servidor A envía una consulta iterativa a B.
- El servidor B refiere a A otro servidor de nombres, incluyendo a C.
- El servidor A envía una consulta iterativa a C.
- El servidor C refiere a A otro servidor de nombres, incluyendo a D.
- El servidor A envía una consulta iterativa a D.
- El servidor D responde.
- El servidor A regresa la respuesta al resolver.

- El resolver entrega la resolución al programa que solicitó la información.

Funcionamiento real del DNS

Los usuarios generalmente no se comunican directamente con el servidor DNS: la resolución de nombres se hace de forma transparente por las aplicaciones del cliente (por ejemplo, navegadores, clientes de correo y otras aplicaciones que usan Internet). Al realizar una petición que requiere una búsqueda de DNS, la petición se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer ninguna comunicación, comprueba si la respuesta se encuentra en la memoria caché. En el caso de que no se encuentre, la petición se enviará a uno o más servidores DNS.

La mayoría de usuarios domésticos utilizan como servidor DNS el proporcionado por el proveedor de servicios de Internet. La dirección de estos servidores puede ser configurada de forma manual o automática mediante DHCP. En otros casos, los administradores de red tienen configurados sus propios servidores DNS.



Tipo de registros DNS

- **A** = Address – (Dirección) Este registro se usa para traducir nombres de hosts a direcciones IP.

- **CNAME** = Canonical Name – (Nombre Canónico) Se usa para crear nombres de hosts adicionales, o alias, para los hosts de un dominio. Es usado cuando se están corriendo múltiples servicios (como ftp y Web Server) en un servidor con una sola dirección ip. Cada servicio tiene su propia entrada de DNS (como ftp.ejemplo.com. y www.ejemplo.com.). esto también es usado cuando corres múltiples servidores http, con diferentes nombres, sobre el mismo host.

- **NS** = Name Server – (Servidor de Nombres) Define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio. Cada dominio se puede asociar a una cantidad cualquiera de servidores de nombres.

- **MX (registro)** = Mail Exchange – (Registro de Intercambio de Correo) Asocia un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

- **PTR** = Pointer – (Indicador) También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en nombres de dominio.

- **SOA** = Start of authority – (Autoridad de la zona) Proporciona información sobre la zona.

- **HINFO** = Host INFOrmation – (Información del sistema informático) Descripción del host, permite que la gente conozca el tipo de máquina y sistema operativo al que corresponde un dominio.

- **TXT** = TeXT - (Información textual) Permite a los dominios identificarse de modos arbitrarios.

- **LOC** = LOCalización - Permite indicar las coordenadas del dominio.

- **WKS** - Generalización del registro MX para indicar los servicios que ofrece el dominio. Obsoleto en favor de SRV.

- **SRV** = SeRVicios - Permite indicar los servicios que ofrece el dominio. RFC 2782

- **SPF** = Sender Policy Framework - Ayuda a combatir el Spam. En este record se especifica cual o cuales hosts están autorizados a enviar correo desde el dominio dado. El servidor que recibe consulta el SPF para comparar la IP desde la cual le llega, con los datos de este registro.

4.7 Servidores radius

Tal y como se indica en *[5]*, RADIUS (Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red o Network Access Server (NAS)) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor

autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

Por lo tanto, el servidor radius permite el funcionamiento centralizado de datos como la certificación, nombres de usuario y contraseñas. En el servidor RADIUS se pueden acumular estos datos certificados a nivel local pero también puede almacenar datos de autenticación, al aire libre en una base de datos SQL externa, o incluso un archivo de UNIX. De hecho, la utilización de un servidor radius es una muy buena opción para llevar a cabo la contabilidad sin ningún tipo de molestia.

4.8 Servidor de NTP

Como se puede leer en *[7]*, los servidores NTP son una herramienta vital para cualquier empresa que necesita comunicarse globalmente y de manera segura. Los servidores NTP distribuyen el Tiempo Universal Coordinado (UTC), el calendario global mundial basado en la hora altamente precisa indicada por los relojes atómicos.

NTP (Network Time Protocol) es el protocolo usado para distribuir el tiempo UTC a través de una red, así como también asegura que toda la hora sea exacta y estable. Sin embargo, existen muchas dificultades en la creación de una red NTP, a continuación las más comunes:

Conseguir la fuente de tiempo más adecuada es fundamental en la creación de una red NTP. La fuente de tiempo va a ser distribuida entre todas las máquinas

y dispositivos en una red por lo que es vital que no sólo sea precisa, sino también estable y segura.

Muchos administradores de sistemas hacen recortes con una fuente de tiempo. Algunos deciden utilizar una fuente de tiempo basados en Internet, a pesar de que no son seguras ya que el firewall requerirá una apertura, sumado a que muchas son enteramente inexactas o se encuentran demasiado lejos de ofrecer cualquier tipo de precisión.

Existen dos métodos de alta seguridad para la recepción de una fuente de tiempo UTC. El primero es utilizar la red de GPS que, aunque no transmite UTC, la hora GPS se basa en el tiempo atómico internacional, con lo cual resulta fácil de convertir para el NTP. Las señales de tiempo GPS son también de fácil acceso a nivel mundial.

El segundo método es utilizar las señales de radio transmitidas por algunos laboratorios nacionales de física. Estas señales, sin embargo, no están disponibles en todos los países, además tienen un rango limitado y son susceptibles a la interferencia y la topografía local.

Los niveles de estrato describen la distancia entre un dispositivo y el reloj de referencia. Por ejemplo un reloj atómico basado en un laboratorio de física o satélite GPS es un dispositivo de estrato 0. Un dispositivo estrato 1 es un servidor de hora que recibe la hora de un dispositivo estrato 0 por lo que cualquier servidor NTP dedicado es estrato 1. Los dispositivos que reciben el tiempo de servidores de hora, tales como ordenadores y routers son dispositivos estrato 2.

El NTP puede soportar hasta 16 niveles de estrato y aunque haya un descenso en la precisión, mientras más se aleje los niveles de estrato están diseñados para permitir que redes de gran tamaño reciban la hora de un solo servidor NTP sin causar congestión en la red o un bloqueo en el ancho de la banda.

Cuando se utilice un servidor NTP es importante no sobrecargar el dispositivo con las solicitudes de tiempo de tal manera que la red deba ser dividida con un número escogido de máquinas que tomen solicitudes del servidor NTP (el fabricante del servidor NTP puede recomendar el número de peticiones que puede manejar). Estos dispositivos estrato 2 pueden entonces ser utilizados como referencias de tiempo para otros dispositivos (que se convierten en dispositivos de estrato 3) en redes muy grandes éstos se pueden utilizar como referencias de tiempo a sí mismos.

Modo de funcionamiento y de operación

Como indican desde *[8]*, NTP es un protocolo basado en un sistema cliente-servidor. Provee a los clientes con tres productos fundamentales: clock offset, round-trip delay y referencia de dispersión. El offset especifica la diferencia entre la hora del sistema local y la referencia externa de reloj. Round-trip delay especifica las latencias de tiempo medidas durante la transferencias de paquetes dentro de la red. La referencia de dispersión de tiempo especifica el máximo número de errores asociados con la información de tiempo recibido de un reloj externo.

El protocolo NTP usa el protocolo UDP el cual es una parte integrada de la pila TCP/IP. Actualmente, la versión actual que se está utilizando es NTP 4 (con la versión 5 en fase de desarrollo, siendo fuente abierta y libremente disponible para su descarga a través de ntp.org), y todas las versiones son compatibles entre sí, La única modificación entre la versión 3 y 4 es una variación en la cabecera para acomodar IPv6.

Un servidor NTP stratum 1 tiene tres modos de operación. Unicast, anycast y multicast. El cliente inicia los modos unicast y anycast, y el servidor responde con un mensaje de tiempo NTP con el que el cliente se sincroniza. Multicast es un modo de envío de mensajes a solo ciertos elementos de la red, a diferencia

de broadcast, el cual habla con todos. A periodos regulares, el dominio es inundado por estos mensajes con motivos de sincronización.

4.9 Gestor de ancho de banda

Tal y como se indica en *[9]*, permite establecer un ancho de banda mínimo y máximo para un tipo concreto de tráfico. El ancho de banda (también *traffic control* o *traffic shaping*) de la red puede garantizarse para los servicios esenciales durante los períodos de alta congestión. Por lo tanto, en caso de saturación, ese tipo de tráfico disfruta del ancho de banda asignado y no nota esa congestión. Es muy recomendado asegurarse que las aplicaciones y recursos críticos reciben una cantidad garantizada del ancho de banda disponible.

La gestión del ancho de banda tiene como objetivo responder a las siguientes cuestiones:

- ¿Quién debería obtener un determinado nivel de servicio para ciertas aplicaciones?
- ¿Qué nivel de prioridad debería asignarse a cada tipo de tráfico?
- ¿Para qué tipo de tráfico debe garantizarse su entrega?
- ¿Qué cantidad de ancho de banda debe ser reservada para garantizar un correcto funcionamiento?

En las redes en las que no se aplica ningún tipo de mecanismo para la gestión del ancho de banda el acceso a aplicaciones críticas puede ser menoscabado, o inclusive inhabilitado, por aplicaciones no críticas; personal bajando o subiendo grandes archivos vía http o ftp u observando aplicaciones multimedia vía Internet. Ciertos servicios de uso regular, pero de menos prioridad, como correos con pesados anexos, larguísimas colas de impresión, tráfico para efectuar respaldos y la copia o transferencia de archivos, sustraen el ancho de

banda disponible y causan congestión en las redes provocando el colapso de aplicaciones críticas. Para evitarlo basta con aplicar políticas de gestión del ancho de banda.

4.10 Sistema de monitorización de equipos

Un sistema de monitorización es aquella solución que puede ayudar a controlar cualquier equipo de una arquitectura de red implantada. Es decir, se puede saber en todo momento el estado de la máquina monitorizada, así como el estado de cualquier servicio que dicha máquina proporciona, pudiendo actuar de manera inmediata en el caso de que se produjera algún tipo de fallo.

En caso de producirse cualquier fallo, se podrá optar por varias maneras de advertir el hecho, ya sea reportándolos vía email, SMS, mensaje instantáneo y/o solucionándolos automáticamente antes de que el cliente o usuario final pueda darse cuenta de los mismos.

Como se puede ver en *[10]*, hay tres valores técnicos fundamentales a la hora de elegir un sistema de monitorización adecuado para nuestro entorno, independientemente del precio o facilidad de instalación y de utilización. Estos tres valores son:

- Forma de presentar los datos, las alarmas y gráficos para su estudio. Estos han de ser lo más eficientes posible y ofrecer una idea de los problemas de un solo vistazo.

- Ubicación, distancia entre equipos y tipo de conexión (velocidad y rendimiento). A más distancia y cantidad de equipos, así como con conexiones lentas, es conveniente utilizar agentes locales que reporten a un servidor central.

- Sistemas Operativos que se monitorizarán. Es más sencillo monitorizar únicamente máquinas basadas en Linux, aunque en la mayoría de los casos es fundamental hacerlo con Windows y conveniente utilizar WMI, (además de SNMP).

Por lo tanto se puede decir, que es fundamental que cualquier sistema de seguridad perimetral que se precie, cuente con un sistema de monitorización para saber en todo momento el estado de todos los equipos que lo componen.

4.11 Sistemas de realización de backups

Como se indica en *[11]*, las copias de seguridad son un proceso que se utiliza para salvar toda la información, es decir, un usuario, quiere guardar toda la información, o parte de la información, de la que dispone en el PC hasta este momento, realizará una copia de seguridad de tal manera, que lo almacenará en algún medio de almacenamiento tecnológicamente disponible hasta el momento como por ejemplo cinta, DVD, BluRay, en Internet o simplemente en otro Disco Duro, para posteriormente si pierde la información, poder restaurar el sistema.

La copia de seguridad es útil por varias razones:

- Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema)

- Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos).

- En el mundo de la empresa, además es útil y obligatorio, para evitar ser sancionado por los órganos de control en materia de protección de datos. Por ejemplo, en España la Agencia Española de Protección de Datos (AEPD).

Normalmente las copias de seguridad se suelen hacer en cintas magnéticas, si bien dependiendo de lo que se trate podrían usarse disquetes, CD, DVD, discos ZIP, JAZ o magnético-ópticos, pendrives o pueden realizarse sobre un centro de respaldo remoto propio o vía internet.

La copia de seguridad puede realizarse sobre los datos, en los cuales se incluyen también archivos que formen parte del sistema operativo. Así las copias de seguridad suelen ser utilizadas como la última línea de defensa contra pérdida de datos, y se convierten por lo tanto en el último recurso a utilizar.

Las copias de seguridad en un sistema informático tienen por objetivo el mantener cierta capacidad de recuperación de la información ante posibles pérdidas. Esta capacidad puede llegar a ser algo muy importante, incluso crítico, para las empresas.

El crecimiento exponencial de los datos, la reducción de las ventanas de backup, y la necesidad cada vez mayor de restaurar los datos en tiempos mínimos, son requisitos a los que todas las empresas se ven sujetas, y que están convirtiendo el proceso de backup y restauración de datos en un desafío para los responsables de los departamentos de sistemas.

4.12 Bastionado de equipos

Todos los esfuerzos en el diseño y despliegue de una plataforma de seguridad perimetral, se centran en ofrecer un servicio requerido, reduciendo al mínimo el riesgo intrínseco de la infraestructura implantada y protegida. Entendiendo el riesgo intrínseco como el producto del impacto asociado al activo por la probabilidad de explotación de las vulnerabilidades existentes en dicho activo.

De manera evidente, sólo se disponen de dos posibilidades para reducir el riesgo, reducir el impacto o reducir la vulnerabilidad del mismo.
Disminuir el impacto supondría reducir el valor del activo o la amenaza existente. Evidentemente sólo queda bajo nuestro control el valor del activo, que para disminuirlo, sólo podemos eliminar o modificar algunos de los servicios ofrecidos o información existente en el activo.

Este último aspecto es uno de los que se ha mantenido a lo largo de este documento, situando únicamente los servicios e información cuyo riesgo pueda asumirse en función de los servicios prestados.

Alternativamente podemos reducir el riesgo intrínseco mediante la disminución de la probabilidad de explotación de las vulnerabilidades existentes en el sistema, para ello se ha justificado ampliamente la necesidad de disponer de sistemas de monitorización y barreras que impidan, en la medida que nos ofrece la tecnología y nuestra experiencia, el acceso a los recursos de manera no autorizada.

Desgraciadamente, pese a la gran efectividad de las barreras de seguridad perimetral, no nos ofrecen soluciones en servicios expuestos a redes públicas por requisitos del servicio (como es el caso de servidores Web, SMTP, etc.). Para estos activos deberemos perseguir con los medios a nuestro alcance el reducir al mínimo las posibilidades de intrusión, su impacto y propagación al resto de elementos de la infraestructura.

Como herramienta básica para lograr este fin, disponemos del bastionado o configuración segura de dispositivos, sistemas operativos y aplicaciones.

Cada sistema requiere un procedimiento de bastionado distinto en función de los elementos que incluya, con lo que escapa a la finalidad de este documento la especificación del procedimiento para cada uno de los casos. No obstante, sí podemos esbozar las directrices básicas del proceso de bastionado y

configuración segura que se deberían aplicar a cada uno de los sistemas a implantar, junto con los equipos Proxy/caché actualmente en servicio:

1. Reducción y control de puntos de acceso a los sistemas.
   - De forma remota.
   - De forma local.

2. Reducción y control de permisos.
   - A usuarios.
   - A aplicaciones.
   - A la información y recursos.

3. Activación de la monitorización de los sistemas
   - Accesos al sistema.
   - Acceso a aplicaciones.
   - Acceso a la información y recursos.

4. Prevención frente a ataques comunes.
   - A nivel de comunicaciones de Red.
   - A aplicaciones.
   - Por configuraciones por defecto o innecesariamente permisivas.
   - Por revelación de información sensible de forma innecesaria.

5. Protección mediante herramientas legales
   - Mostrado de condiciones de uso.
   - Tratamiento de la información.

De esta forma prácticamente se duplica el grado de seguridad del sistema y consecuentemente el valor de la inversión realizada.

5. DESCRIPCIÓN EXPERIMENTAL

5.1 Requisitos del cliente

En este apartado se repasan los requisitos expresados por la empresa ficticia, a partir de ahora llamada SEGURAMA (una aseguradora), para la implantación de un entorno de seguridad perimetral, en los que se basará para proponer una buena solución.

Requisitos de la arquitectura de Seguridad

1. Arquitectura de seguridad perimetral con dos niveles de cortafuegos, de fabricantes y tecnologías distintos. Cada nivel se configurará en un cluster de cortafuegos redundante en modo activo – activo, con balanceo de carga.

2. Detrás del primer nivel de cortafuegos se implementarán subredes apantalladas para configurar una o varias DMZ donde se ubicarán los servidores de acceso público de SEGURAMA.

3. La arquitectura propuesta deberá contemplar y justificar la ubicación lógica de las siguientes zonas de seguridad, además de detallar el modelo de filtrado y mecanismos de seguridad previstos en las mismas:

   - Zona de servidores públicos: incluye servidores Web, servidores de DNS y frontales de correo (se admite una segmentación mayor).
   - Zona de servidores Proxy
   - Zona de LAN de usuarios de Servicios Centrales
   - Zona de gestión de la plataforma de seguridad

- Zona de servicios internos: incluye servidores internos de SEGURAMA, bases de datos, controladores de dominio, servidores de aplicaciones, Intranet, correo, etc.

4. El diseño ofertado perseguirá en todo momento cumplir con una filosofía de seguridad basada en el concepto de defensa en profundidad, lo que implicará un bastionado de cada elemento de seguridad.

Requisitos de los elementos de seguridad

5. Se deberá incluir en la oferta un número suficiente de cortafuegos para cumplir con las exigencias de la arquitectura demandada en el punto anterior.

   Además cada nivel deberá ofrecer las siguientes prestaciones mínimas:

   - Throughput de 1 Gb/s para el primer nivel y 800 Mb/s para el segundo.
   - Un mínimo de 8 interfaces de red en cada cortafuegos, donde 4 de ellos deberán estar configurados a 1 Gb/s.

   Detrás del primer cortafuegos se implementará una subred apantallada para configurar una DMZ.

6. La solución deberá aportar obligatoriamente las sondas de detección de intrusión de red que se consideren necesarias, especificando en todo caso en qué segmentos y subredes se sitúan y por qué motivo, además de los procedimientos y mecanismos de calibración de las mismas.

7. Se requerirá el suministro de al menos 4 sondas de detección de intrusión de host o soluciones de cortafuegos personales para sistemas operativos Windows, Linux o HP-UX, que irán destinadas a la monitorización de los equipos más críticos de la red.

8. Se considera necesario contemplar el suministro y configuración de tecnología antivirus y anti-spam de correo para los servidores del frontal de correo y tecnología antivirus de navegación web, de fabricantes distintos a las soluciones antivirus actuales de SEGURAMA, que son del fabricante Panda Security.

9. Se deberá suministrar algún elemento de seguridad que posibilite el control de acceso y contenidos en la navegación web de los usuarios de SEGURAMA.

10. Se requiere la provisión de un gestor de ancho de banda con el objetivo de permitir la gestión del tráfico y comunicaciones entre SEGURAMA e Internet (en ambos sentidos) y que permita controlar y priorizar dicho tráfico en función de parámetros como tipo de protocolo, servidor origen o destino, dirección IP, etc.

    Además actuará como un elemento de seguridad adicional al configurarse adecuadamente para evitar ataques de denegación de servicio.

11. Será necesario dotar a la red de algún elemento de seguridad, tipo servidor radius, para poder realizar conexiones segura desde el exterior de la red mediante dispositivos móviles como puedan ser PDA´s o portátiles, utilizando para ello tarjetas de telefonía móvil.

12. Acorde con el punto anterior, también se deberá poder acceder de forma segura a la red interna mediante una conexión ADSL normal. Esta

comunicación deberá realizarse mediante un cifrado que asegure la integridad de todos los datos que salgan de la organización.

13. Para la gestión de todos los elementos de seguridad, se contará con una plataforma completa de gestión que se ubicará en un segmento de red separado e incluirá como mínimo los siguientes elementos:

    - Consolas y servidores necesarios.
    - Herramientas de gestión y monitorización de todos los elementos de seguridad aportados.

    La plataforma de gestión deberá de estar convenientemente securizada.

14. En relación al requisito anterior, se deberá proporcionar una solución que monitorice en tiempo real cada uno de los elementos de seguridad, avisando si fuese necesario la caída o mal funcionamiento de cualquiera de ellos.

Requisitos de servidores y elementos físicos adicionales

15. La solución ofertada a SEGURAMA deberá contemplar la provisión de los siguientes servidores, junto con su instalación y configuración, considerados imprescindibles para completar el entorno de seguridad perimetral:

    - Servidores y consolas necesarios para la gestión completa del entorno de seguridad perimetral.
    - Servidores para DNS público, para la resolución de nombres del dominio de SEGURAMA publicados hacia Internet.
    - Servidores para frontal o pasarela de correo electrónico con conexión a los servidores de correo interno con los que actualmente cuenta

SEGURAMA (plataforma Intel con S.O. Windows Server 2008 y Exchange Server 2010).

16. En la oferta se deberá incluir además, todos los elementos físicos adicionales necesarios para construir la infraestructura de seguridad perimetral como por ejemplo racks, cableado de conexión de red y alimentación eléctrica, armarios, etc.

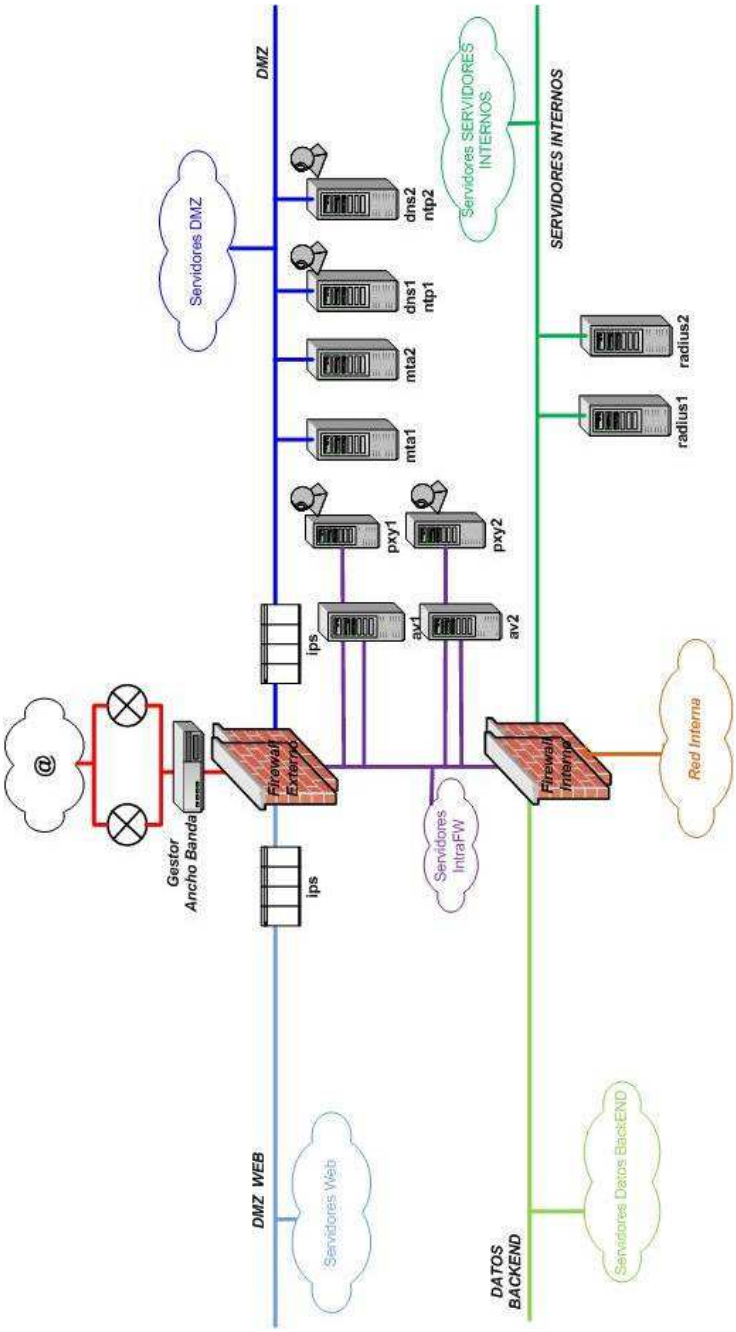
Requisitos de documentación y gestión de la plataforma

17. Como parte del proyecto de implantación, se deberá proporcionar a SEGURAMA toda la documentación que se derive del mismo, incluyendo:

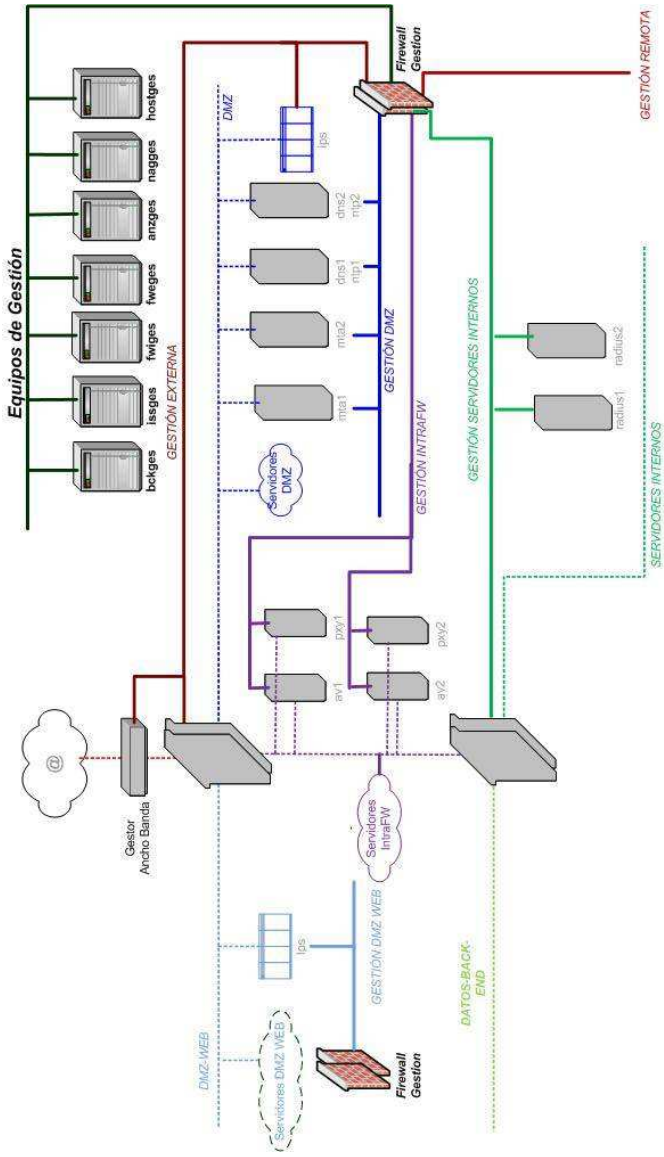
- Diagramas lógicos y físicos de la arquitectura proporcionada, elementos de seguridad suministrados y esquemas de red del entorno de red (segmentación, direccionamiento IP, etc.).
- Documentos de configuración de equipos, servidores, reglas de cortafuegos, software instalado, parches, etc.
- Procedimientos de monitorización y gestión de la seguridad incluyendo: procedimientos de actuación ante incidencias, procedimientos de realización de cambios físicos y lógicos en la red, procedimientos de configuración de servidores en el entorno de seguridad perimetral.
- Descripción detallada de los trabajos periódicos de gestión a realizar por el personal aportado, con un desglose temporal a nivel de día, semana y mes.
- Manuales de uso de las herramientas de gestión y de los elementos de seguridad.

5.2 Implantación y adecuación de los elementos de seguridad en la empresa

Mapa topológico de la red de servicio



Mapa topológico de la red de gestión



- ***bckges:*** Servidor de backup donde se hacen las copias de seguridad de los elementos de seguridad.
- ***issges:*** servidor de gestión de las sondas de host
- ***fwiges:*** servidor de gestión del Firewall Interno
- ***fweges:*** servidor de gestión del Firewall Externo
- ***anzges :*** servidor de gestión de las sondas de red

- ***nagges:*** servidor nagios
- ***hostges:*** servidor donde se instalan todos las interfaces gráficas para gestionar las distintas management.

Direccionamiento IP

Redes de servicio:

DMZ: 192.168.220.0/24
DMZ WEB: 192.168.228.0/24
DATOS BACKEND: 192.168.230.0/24
SERVIDORES INTERNOS: 192.168.224.0/23
SERVIDORES INTRAFW: 192.168.222.0/25
RED INTERNA: 192.168.4.0/22

Redes de gestión:

GESTIÓN DMZ: 192.168.238.0/25
GESTIÓN DMZ WEB: 192.168.238.128/25
GESTIÓN SERVIDORES INTERNOS: 192.168.236.128/25
EQUIPOS DE GESTIÓN: 192.168.236.0/25
GESTIÓN INTRAFW: 192.168.222.128/25
GESTIÓN EXTERNA: 192.168.223.0/25
GESTIÓN REMOTA: 192.168.244.0/23

Descripción de cada una de las soluciones elegidas para cada elemento de seguridad

A continuación se irán presentando cada una de las soluciones comerciales que se han elegido para formar esta arquitectura de seguridad perimetral. Se irán presentando en orden de más fuera del perímetro hacia más adentro, y por cada una de ellas, se expondrá otra alternativa.

RED EXTERNA

Gestor de ancho de banda

Solución de mercado elegida

Allot NetEnforcer AC-1400

Características

La solución de Allot NetEnforcer AC-1400 viene dada en el siguiente appliance:

Se elige este modelo de Allot por su capacidad de throughput, ya que se adecua al que tendrá la empresa.

Sus características fundamentales son las siguientes *[12]*:

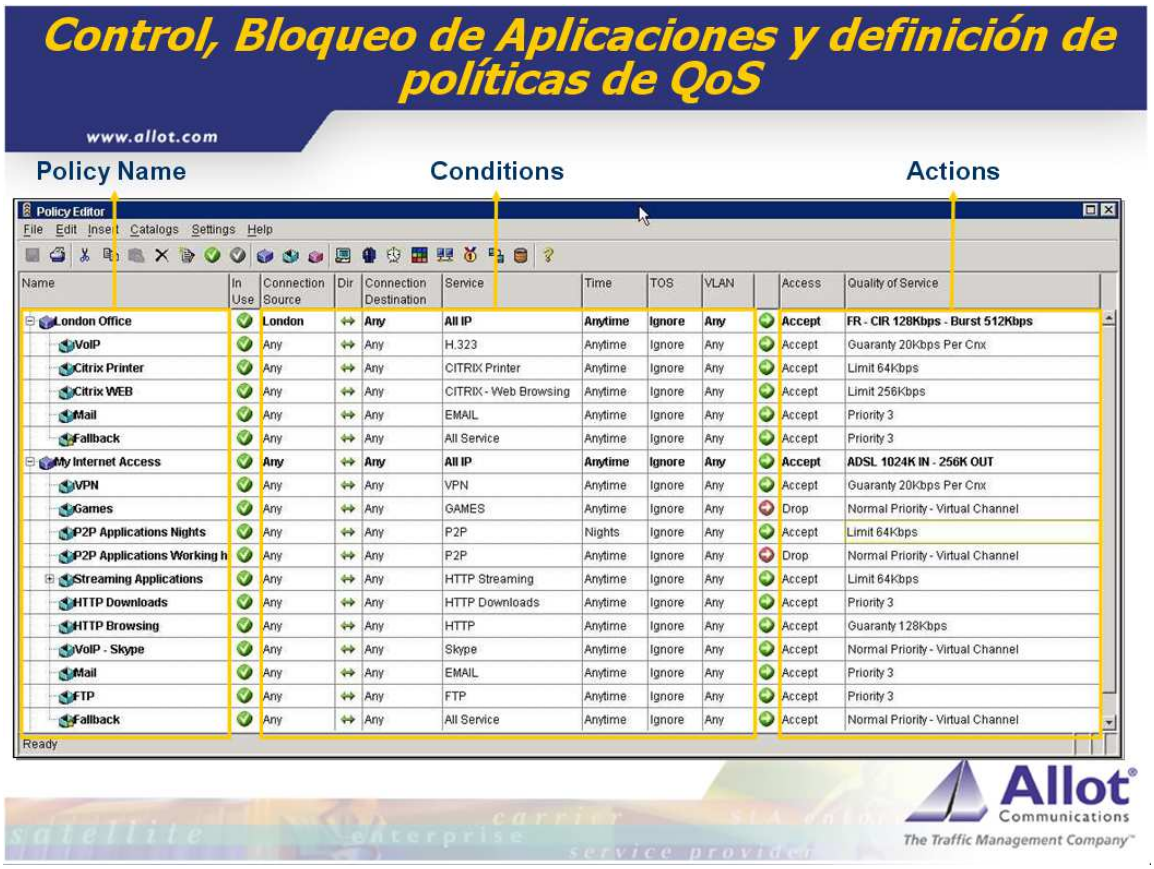
- 8 x 1GE ports for network connectivity
- 4 x 1GE ports for connectivity to external service systems
- Scalable throughput ranging from 45Mbps to 1Gbps full duplex
- Real-time monitoring and QoS policy enforcement for up to 4 million concurrent IP flows
- Traffic steering
- Powered by Allot's Dynamic Actionable Recognition Technology (DART)
- DART's extensive signature library accurately identifies hundreds of Internet applications and protocols, including P2P, VoIP, video, streaming, gaming, instant messaging, web and business applications
- Automated, web-based update of protocol/signature library
- Proactive alarms
- Fail-safe performance with external bypass
- Centralized Allot NetXplorer management
- Full Integration with network & subscriber services
- Allot SMP Subscriber Management and subscriber-application control.
- Allot WebSafe URL filtering solutions.
- Allot MediaSwift Video acceleration & P2P caching solutions.
- Allot Service Protector for botnet and DDoS detection and mitigation.

Los aspectos más importantes de esta solución son los siguientes:

- Visibilidad completa de la aplicación, usuarios y el tipo de tráfico de red.
- Control de coste por la gestión del ancho de banda y el uso eficiente de la red.

- Mejora de la experiencia del usuario incluyendo los servicios más utilizados.
- Aumentar el ARPU a través de jerarquización de servicios y las políticas de gestión de cuotas.
- Protección del negocio con informes y resolución de problemas en tiempo real.

A continuación se mostrarán unas capturas de pantalla para hacerse una idea de cómo es la consola y la gestión de este producto:



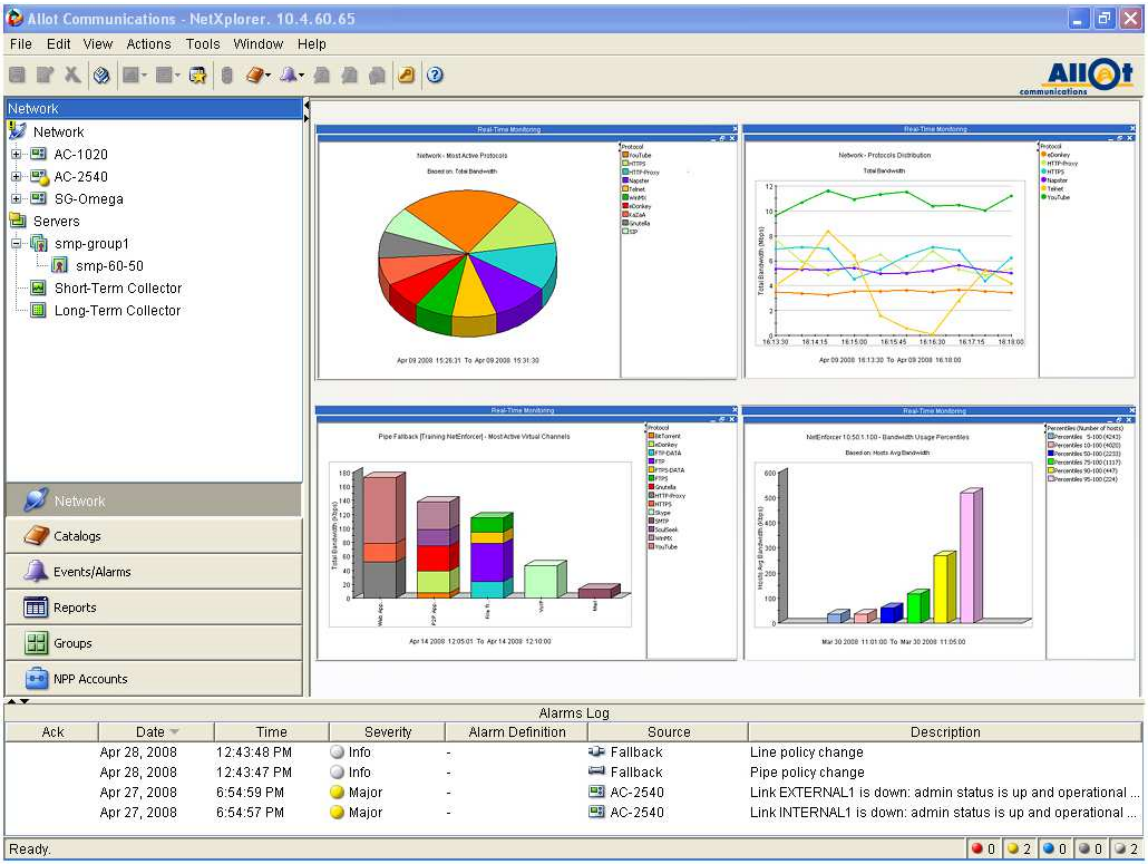
Para gestionar escenarios en los que se encuentren desplegados varios dispositivos NetEnforcer existe un software que se puede instalar en cualquier servidor (siempre que cumpla los requisitos necesarios), llamado NetXplorer. Este servidor será un complemento perfecto para la monitorización, gestión y realización de reportes de todos los dispositivos en una consola centralizada.

A continuación se enumeran algunas de las características más importantes:

- Configuración centralizada de todos los dispositivos y plataformas administrados
- Monitorización en tiempo real y realización de reportes de consumo de ancho de banda.
- Informes de larga duración.

- Informes de datos ilimitados.
- Gran conjunto de informes con múltiples estilos gráficos y gran variedad de filtros para mostrar de forma más granular.
- Facilidad para personalización y programación de informes recurrentemente.
- Gran variedad de políticas de QoS por aplicación, usuario y tipo de red.
- Planes de aprovisionamiento de servicios.
- Servicio de medición.
- Interfaz con múltiple formato de datos para exportar.
- Alarmas inteligentes.
- GUI de fácil manejo.

En este gráfico se observa cómo es la consola del NetXplorer:



Alternativas

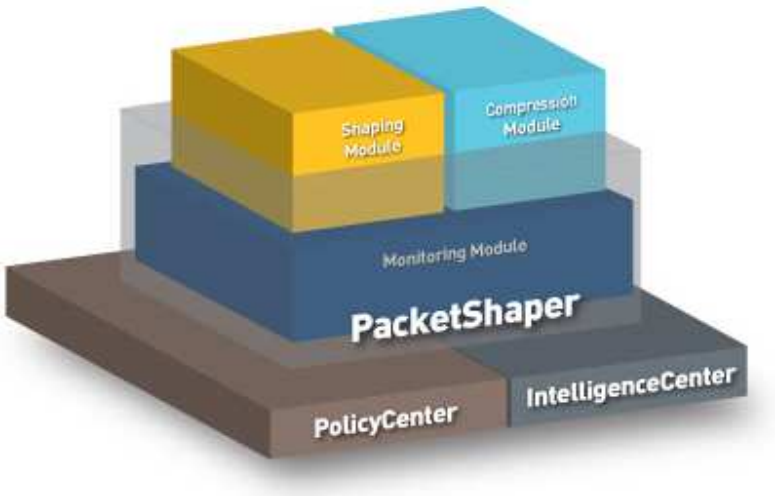
La alternativa elegida es PacketShaper, de la compañía Blue Coat.

A continuación se mostrará una tabla, sacada de *[13]*, en la que se pueden ver todos los modelos que se encuentran actualmente en el mercado, especificando en cada uno de ellos las características fundamentales:

PACKETSHAPER SERIES	900	1700	3500	7500	10000 | 10000 ISP****	12000 | 12000 ISP****
Maximum Capacity						
IP Flows (TCP)*	5,000	30,000	40,000	200,000	300,000 | 900,000	450,000 | 1,300,000
IP Flows (UDP)*	2,500	15,000	20,000	100,000	150,000 | 360,000	225,000 | 500,000
Classes	256	512	1,024	1,024	2,048 | 5,000	2,048 | 5,000
Dynamic Partitions	**	1,024	1,024	10,000	20,000 | 20,000	20,000 | 20,000
Static Partitions	128	256	512	512	1,024 | 5,000	2,048 | 5,000
Shaping Policies	256	512	1,024	1,024	2,048 | 5,000	2,048 | 5,000
Max # of Matching Rules	640	2,562	2,562	5,120	5,000 | 12,500	12,500 | 20,000
IP Hosts*	5,000	15,000	20,000	150,000	200,000 | 400,000	300,000 | 600,000
Active Tunnels	10	15	30	100	1,000 | N/A	1,000 | N/A
Software Options and Upgrades						
Monitoring Only	Yes	Yes	Yes	Yes	Yes	Yes
Link Speeds with Shaping Options	512 Kbps 2 Mbps — —	2 Mbps 6 Mbps 10 Mbps —	2 Mbps 6 Mbps 10 Mbps 45 Mbps	10 Mbps 45 Mbps 100 Mbps 200 Mbps	100 Mbps 200 Mbps 310 Mbps —	500 Mbps 1 Gbps No limit ***** —
Compression***	2 Mbps	10 Mbps	20 Mbps	45 Mbps	155 Mbps | N/A	155 Mbps | N/A
Interfaces						
Onboard Ports (Pairs)	Copper: 2x10/100 Mbps	Copper: 1x10/100/1000 Mbps	Copper: 1x10/100/1000 Mbps	Copper: 1x10/100/1000 Mbps	Copper: 1x10/100/1000 Mbps Or, Fiber: 1x1000 Mbps	Copper: 1x10/100/1000 Mbps
LAN Expansion Modules	Backup fail-to-wire pair built in	N/A	Up to 2 dual-port modules Copper: 10/100/1000 Mbps Fiber: SFP	Up to 2 dual-port modules Copper: 10/100/1000 Mbps Fiber: SFP	Up to 2 dual-port modules Copper: 10/100/1000 Mbps Fiber: SFP	Up to 1 dual-port module Copper: 10/100/1000 Mbps Fiber: SFP Copper: 10 Gbps Or, up to 1 four-port module Copper: 10/100/1000 Mbps Fiber: SFP
Out of Band Management	Through backup ports	Yes	Yes	Yes	With LEM	Yes, + Direct Standby port
Console Port	All have RS-232 (AT-compatible) with male DB-9 connectors					
Dimensions (All are 19 in. rack mountable)						
Height	1U (1.75 in/4.45 cm)	1U (1.75 in/4.45 cm)	2U (3.5 in/8.89 cm)	2U (3.5 in/8.89 cm)	2U (3.5 in/8.89 cm)	1U (1.69 in/4.30 cm)
Width	8.66 in (22.00 cm)	17 in (43.18 cm)	17.35 in (44.07 cm)	17.35 in (44.07 cm)	17.31 in (43.97 cm)	16.93 in (43.0 cm)
Depth	9.68 in (24.60 cm)	14 in (35.56 cm)	16 in (40.64 cm)	16 in (40.64 cm)	20.25 in (51.43 cm)	27.44 in (69.70 cm)
Weight	4.50 lbs (2.05 kg)	14 lb (6.35 kg)	18.04 lb (8.18 kg)	20.48 lb (9.29 kg)	33 lb (14.97 kg)	36.5 lb (16.5 kg)
Power						
Power Supply	100/240 VAC; 50/60 Hz, 2 A	100/240 VAC; 50/60 Hz, 2.5 A	100/240 VAC; 50/60 Hz, 2.5 A	100/240 VAC; 50/60 Hz, 2.5 A	100/240 VAC; 50/60 Hz, 6 A	100/240 VAC; 50/60 Hz, 6 A
Dual, Redundant Load Sharing	No	No	No	Yes; Hot-swappable	Yes; Hot-swappable	Yes; Hot-swappable
Additional Features						
Interoperability	XML, XML and CGI APIs, SNMP MIB, SNMP event traps, HP OpenView, infoVista, CA eHealth, IBM Tivoli, Micromuse Netcool					
Device Management	Console access, Web browser interface, Telnet CLI, SNMP Blue Coat MIB and MIB-II support					
Agency Approval						
Safety	IEC 60950-1; EN 60950-1+A11, CAN/CSA-C22.2 No. 60950-1:03; UL 60950-1:03; EN 60825-1,-2 Class 1 Laser					
EMC/EMI	AS/NZS 3548 Class A; AS/NZS 4252.1; ICES-003 Class A; EMC Directive 89/336/EEC; EN 300 386 v1.3.1: 2001 Telecom EMC standard; EMC Directive 73/23/EEC; EMC Directive 93/68/EEC; EN 55022: 1998 Class A; EN 61000-3-2: 1995_A1(98) + A2(98), & prA1 4(00); EN 61000-3-3:1:1995; EN 55024:1998; VCCI:2002 Class A; KN55022 Class A; KN6100-4-2,3,4,5,6,8,11; GOST-R 60950-2002; GOST-R 51318.22,.24-99; FCC 47 CFR part 15, subpart B Class A; CNS 13438 Class A					

Con estos datos se puede ver que el modelo que más se adecua con la infraestructura que se va a desplegar es el 7500 dado que es el que cumple con el throughput mínimo requerido.

En este dibujo se pueden ver las capas que forman el producto PacketShaper *[13]*:



Monitoring Module: Descubre y monitoriza más de 700 aplicaciones inspeccionando internamente la capa 7 para dar una imagen exacta de este tipo de tráfico. Además categoriza más de diez millones de sitios Web.

Shaping Module: Garantiza ancho de banda para aplicaciones sensibles a determinada latencia, asigna prioridades a aplicaciones y contenidos Web, y

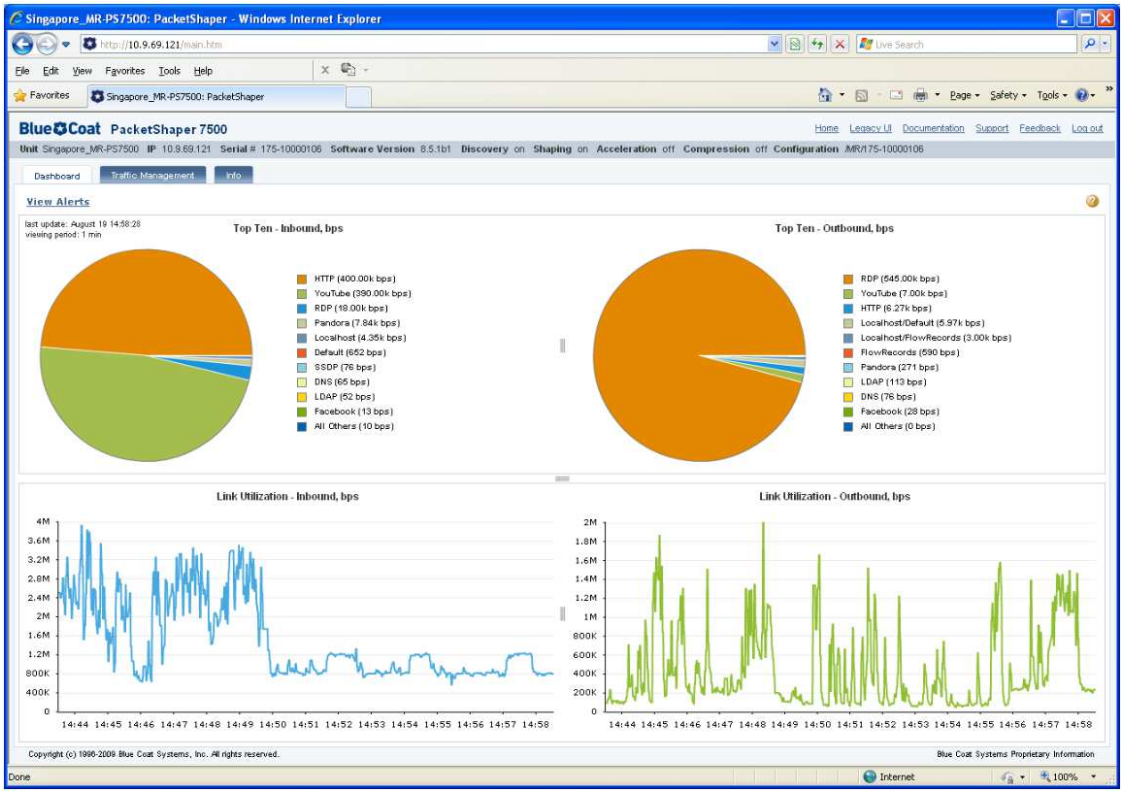
contiene el impacto de tráfico de menor prioridad utilizando un control flexible basado en políticas.

Compression Module: Aumenta la capacidad de la WAN al tiempo que mejora el rendimiento.

PolicyCenter Software: Administra escenarios en los que hay desplegados varias unidades PacketShaper, con una configuración y despliegue de software centralizado.

IntelligentCenter: Simplifica la gestión del rendimiento de aplicación con una monitorización centralizada, realizando análisis de logs e informes de históricos de rendimientos.

En este gráfico se pueden apreciar algunas formas de monitorizar el tráfico:



Firewall externo

Solución de mercado elegida

La solución elegida es **StoneGate de Stonesoft.**

Características

A continuación se van a enumerar algunas de las características más importantes de los cortafuegos de esta marca:

- Elevado rendimiento
- Inspección eficiente
- Facilidad de gestión
- Funciones avanzadas de alta disponibilidad
- Integración para defensa en niveles

El firewall StoneGate dispone de una arquitectura nueva y diferente, que proporciona un nivel de seguridad de red y continuidad de negocio que las aproximaciones tradicionales no pueden ofrecer. Crea un perímetro proactivo alrededor de la empresa, previene ataques, y securiza las comunicaciones de datos con múltiples conexiones paralelas de redes privadas virtuales (VPN).

En concreto se ha optado por el modelo FW-1030 porque cumple con las características que requiere el escenario donde se va a implantar.

Por lo tanto, para la barrera de cortafuegos externos se necesitarán dos appliance FW-1030 con las siguientes características básicas *[14]*:

Licensed Performance	FW-1030	FW-1030P
Firewall throughput	1 Gbps	1.6 Gbps
VPN throughput	140 Mbps	220 Mbps
VPN tunnels	1 000	1 000
Concurrent connections	700 000	900 000
Connections/sec	15 000	15 000
Number of Protected IPs	Unlimited	Unlimited
Concurrent mVPN Clients	25	100
VLANs	150	250
Deep inspection throughput	250 Mbps	250 Mbps
SSL Inspection for client/server	40 Mbps/-	40 Mbps/40 Mbps

Hardware

Network interfaces	
Ethernet	6 x 10/100/1000 copper
Connectors	RS-232 serial console, 2 x USB

Specifications

General	Application level inspection, stateful inspection, packet filtering, circuit level firewall with TCP proxy protocol agent. Integrated operating system.
Firewall protocol agents	FTP, H.323, HTTP, HTTPS, IMAP4, MS RPC, NetBios Datagram, Oracle SQL Net, POP3, RSH, SIP, SMTP, SSH, SunRPC, TCP Proxy, TFTP
VPN Protocols	IKEv1, IPsec
Encryption	AES-128, AES-256, AES-GCM, Blowfish, DES, 3DES*
Message Digest Algorithms	AES-XCBC-MAC, MD5, SHA-1, SHA-256
Diffie-Hellman	DH group 1, 2, 5 and 14
Authentication	RSA and DSS signatures with X.509 certificates, pre-shared keys, hybrid XAUTH
Compression	IPCOMP Deflate
User Authentication	Internal user database, LDAP, MS Active Directory, RADIUS, TACACS+

Features	
High availability	Active/active firewall clustering up to 16 nodes
	Active/standby
	Stateful failover (including VPN connections)
	Server loadbalancing
	VRRP
ISP multihoming	Multi-Link: High availability and load balancing between multiple ISPs including VPN connections
IP address assignment	FW clusters: Static, FW single nodes: static, DHCP, PPPoE, IPv4, IPv6
	Services: DHCP Server and DHCP relay
Traffic management, QoS	Guaranteed & Maximum bandwidth, Priorization, Differentiated Services Code Point (DSCP) matching / marking
SIP	Allows RTP media streams dynamically, NAT traversal, deep inspection, interoperability with RFC3261 compliant SIP devices
SSL inspection	Decrypts the SSL and inspects the HTTP stream protecting web clients and/or servers
Dynamic multicast routing	IGMP proxy

De esta forma, la organización tendrá una primera barrera de protección, que estará dotada de alta disponibilidad ACTIVO-ACTIVO mediante un clúster FW, procesando tráfico ambos nodos, y con la seguridad de que si uno de ellos cae, el otro nodo se encargará de procesar el tráfico total. Este cortafuegos permite conexiones VPN, que valdrán para conectarse de forma segura a la organización desde fuera.

La plataforma fundamental con la que se gestionarán todos los elementos de seguridad es la ***SMC (StoneGate Management Center***). Esta plataforma está formada por al menos tres elementos:

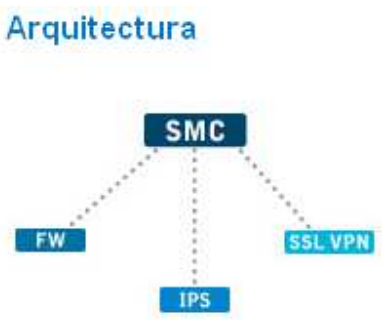
Management server: Esta máquina será la encargada de proporcionar herramientas para la gestión de la seguridad, monitorización y compatibilidad regulatoria.

Con esta management se podrán gestionar todos los elementos de seguridad (IPS, FW y VPN) de StoneGate, centralizando en una misma máquina todas las configuraciones, elementos para realización de reglas, etc.

Log Server: se encarga de la centralización de logs, y normalmente se instala en la misma máquina donde está la Management, de esta forma también se tendrán centralizados todos los logs que aporten tanto los FW, IPS y VPN.

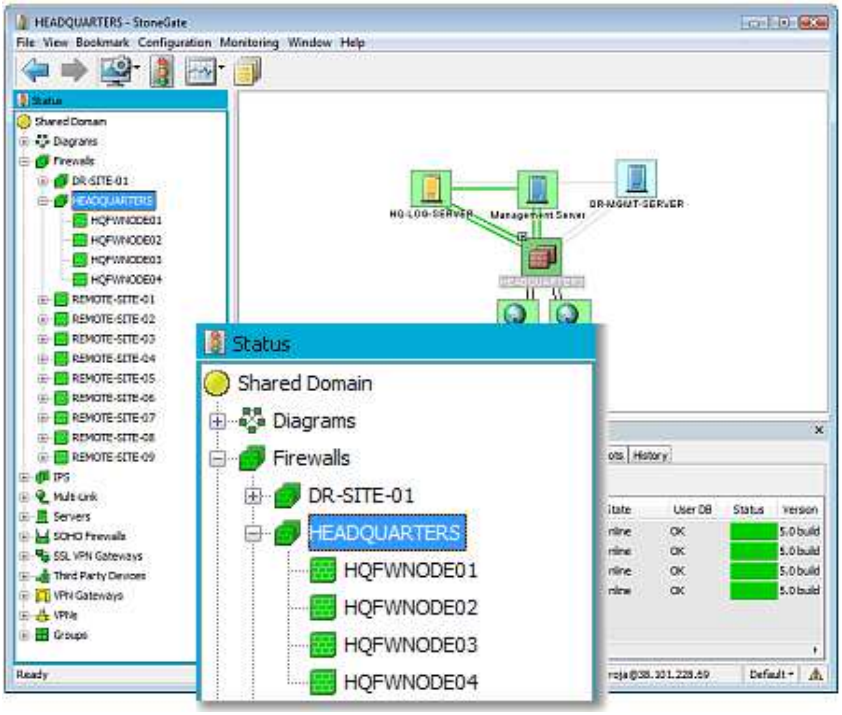
Management Client: Se trata de un software que corre sobre una máquina cualquiera (se puede instalar en varias máquinas), la cual se conecta a la Management Server, y es la consola con la que se realiza toda la configuración que se aplicará a la Management, y ésta a su vez importará a cada elemento de seguridad.

A continuación se muestra la arquitectura de la SMC *[14]*:



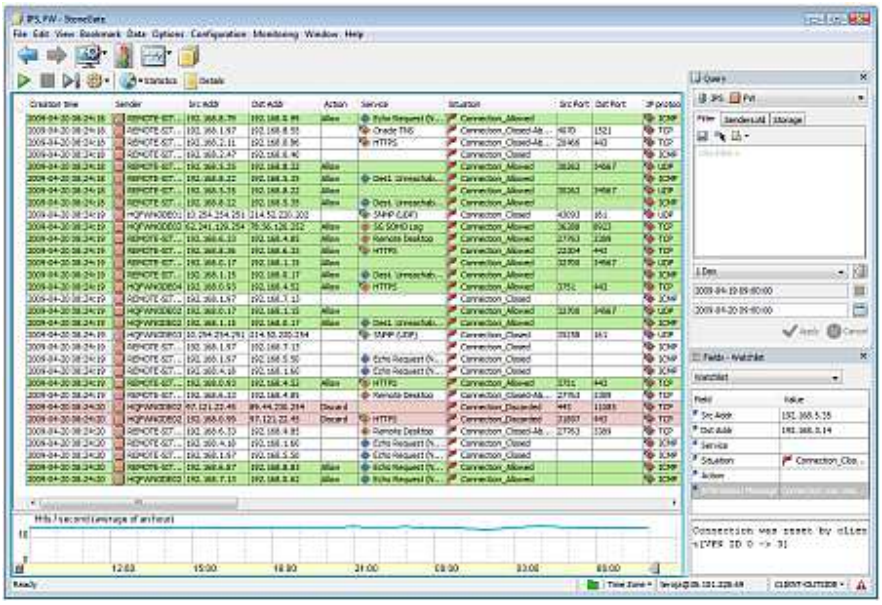
Desde esta consola se realizará toda la configuración y se podrán ver todos los reportes de cada elemento de seguridad, a continuación se muestran unas capturas de pantalla de algunas partes:

Estado de los elementos de seguridad:



Visualización de la red:

Visualización de logs:



Políticas de seguridad del FW:

Access Rules | Inspection Rules | NAT Rules

	ID	Source	Destination	Service	Action
⊟	INBOUND ACCESS FROM INTERNET				
⊞	11.14.13	Internet	$ Local Non Pr	ANY	Jump INBOUN...
	11.14.14	Internet	Web Server NA	HTTP HTTPS	Allow
⊟	OUTBOUND ACCESS FROM SSL-VPN				
⊞	11.14.16	HQSSLVPN	ANY	ANY	Jump OUTBOU...
⊟	DMZ ACCESS FROM INTERNAL				
	11.14.18	$ Local Intern	smc.stonegate	FTP	Allow
⊟	VPN ACCESS - SITE-TO-SITE				
	11.14.20	$ Local VPN N	$ Remote VPN	ANY	Enforce VPN: S..
	11.14.21	$ Remote VPN	$ Local VPN Ne	ANY	Enforce VPN: S..
⊟	VPN-CLIENT				
	11.14.26	$ DHCP Addre	Intenal Networ	ANY	Apply VPN: MO..
	11.14.27	$ DHCP Addre	Intenal Networ	ANY	Apply VPN: MO..

Alternativas

La alternativa que se propone es Check Point, que se trata de otro de los cortafuegos más conocidos y utilizados en el mercado. Se podrán ver todas las características en el apartado de Firewall Interno.

DMZ

Antivirus de correo

Solución de mercado elegida

Esafe Mail Security Gateway, de SafeNet.

Características

Se trata de un antivirus y relay de correo, que servirá para recibir y enviar los correos de la organización, previo escaneo de cada uno de los correos para prevenir que se introduzcan virus, spam, correos de phising, y otro tipos de malware en la organización.

eSafe Mail Security Gateway utiliza un doble motor anti-spam con real-time reputation y análisis profundo de contenido (deep inspection) para bloquear el spam y los ataques de virus con más de 99% tasa de detección.

También dispone de doble motor de antivirus, con una gran base de datos de firmas de virus, spyware y otros malwares, permitiendo al a administrador asignar políticas de seguridad de forma muy granular a usuarios de LDAP, Active Directory y otros grupos.

Esafe Mail Security Gateway se subdivide en cuatro módulos *[15]*:

Security (includes anti-malware, anti-spyware, and anti-virus):

eSafe es capaz de detectar de forma proactiva los intentos de aprovechar las vulnerabilidades antes de que hayan entrado en la organización, en lugar de detectar el malware cuando se está descargando, lo que podría resultar fatal.

Algunas características son las siguientes:

- Doble motor antivirus (Esafe y Kaspersky AV)
- Soporta todo tipo de archivos de MS Office
- Se actualiza automáticamente cada hora
- Soporta filtrado de scripts inteligentes
- Realiza detección de ofuscación
- Detecta y bloquea ficheros conocidos de spyware y sitios web.
- Bloquea canales de comunicación y protocolos utilizados por los spyware.
- Evita que los spyware saquen fuera datos confidenciales de la organización.

Data Leak Prevention (DLP):

Este módulo permite el control de todo el tráfico saliente, denegando la salida de aquel tráfico que se considere que no debería salir de la organización, como pueden ser datos confidenciales, y datos sensibles a que sean conocidos fuera.

El módulo DLP, ayuda a cumplir la legislación vigente, minimiza los falsos positivos y provee de herramientas de descubrimiento y análisis forense.

Estas políticas de DLP, ofrecen una granularidad que puede aplicarse a los distintos grupos existentes en la organización, ya sean de LDAP, AD, y otras, pudiendo generar reportes y alertas cuando se intentan mandar este tipo de datos fuera.

Las nuevas capacidades de clasificación ayudan a los administradores a detectar y prevenir la fuga de datos para determinados tipos de archivo comunes (Unicode, MS Office, PDF, HTML, e-mail, source code files, etc.).

Anti-spam and anti-phishing:

Los dos motores de eSafe anti-spam ofrecen una protección completa, control total, y una mayor productividad. La combinación de estrategias de contención y reputación, permiten que el al módulo de anti-spam unir tecnologías de real-time reputation e inspección profunda en una sola solución integrada.

El uso de dos motores permite la detección del 99% de todos los intentos de spam y phishing, y reduce al mínimo los falsos positivos, asegurando que los usuarios reciben sólo los e-mails relevantes y de confianza. Al ser cada motor de una tecnología diferente, esto permite un ajuste entre ellos y una cobertura completa.

Aquí se enumeran algunas de las principales características:

- Más de un 99% de detección de spam
- Dos motores anti-spam
- Un reporte de emails en cuarentena diario
- Política basada en usuarios
- Única tecnología anti-phishing, que detecta hipervínculos anómalos y ofuscaciones
- Bloqueos de hipervínculos que llevan a la suplantación de identidad o sitios web maliciosos

Management and Reporting:

El módulo de Management and Reporting permite a los administradores funciones avanzadas que les permiten controlar de forma sencilla la red y mantener la política de seguridad de la organización. Este módulo les permite ver en tiempo real todo lo que ocurre en la red, lo que les permite tomar rápidamente medidas cuando la red se ve amenazada o atacada, y proporciona información detallada con un nivel amigable de gestión los informes de uso de Internet.

En este módulo se encuentra el Security Center, que es la consola de administración que permite a los administradores configurar y ejecutar la política de seguridad de contenidos en toda la red.

El Security Center provee estas funciones:

- Gestión centralizada de todas las máquinas eSafe desde un único servidor
- Configuración remota y administración desde cualquier lugar de la organización o de los proveedores de servicios remotos gestionados
- Comunicación autenticada, con una conexión cifrada
- Niveles individuales de protección y reglas que pueden ser definidas de acuerdo a las características específicas (es decir, clientes, servidores, correo electrónico, dominios, remitentes, destinatarios, tipos de archivo, y más), lo que permite el perfeccionamiento de inspección de contenidos y gestión del correo
- Estadísticas en tiempo real que muestran el estado actual del tráfico, se presentan en gráficos de acuerdo al protocolo, extensos informes y alertas para notificar los intentos cada vez que un virus intenta entrar en la red.

A continuación se muestra una captura de pantalla de la consola principal:

Esta solución se implantará sobre un servidor HP DL 120 G7, ya que por especificaciones técnicas cumple con los requisitos necesarios para el servicio.

En estos gráficos se muestran las principales características del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Core™ i3 2100 (2 núcleos, 3,1 GHz, 3 MB, 65 W, 1333/t)
Número de procesadores	1
Núcleo de procesador disponible	2
Memoria, estándar	2 GB
Ranuras de memoria	4 ranuras DIMM
Tipo de memoria	PC3-10600E DDR3 UDIMMs
Ranuras de expansión	2
Controlador de red	(2) 1 puerto NC112i 1 GbE
Tipo de fuente de alimentación	(1) detección automática de 400 W, cumple con la marca CE
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	Ningún estándar de suministro
Formato (totalmente configurado)	1U
Garantía - año(s) (partes/mano de obra/in situ)	1/1/1

Alternativas

La alternativa es Optenet MailSecure.

A continuación se muestran las funcionalidades de esta solución *[17]*:

SEGURIDAD

Seguridad Email: Con una combinación de 16 tecnologías diferentes para el bloqueo de Spam, la solución de Seguridad Email de alto rendimiento de Optenet garantiza al mayor nivel de protección para eliminar y administrar amenazas de correos electrónicos entrantes y salientes.

Filtro de Spam saliente: El filtro de spam saliente impide que los servidores de correo de la organización se usen para la distribución masiva de spam y protege del spam generado en su red por ordenadores infectados y "bots".

Protección contra malware: La Seguridad Email se complementa con el motor antivirus más avanzado de Kaspersky Labs y Sophos, para ofrecer una protección superior frente a virus, spyware, troyanos, gusanos y más.

Antiphishing: MailSecure introduce un motor de antiphishing que analiza tráfico web y email para identificar actividades sospechosas y proteger de ataques de phishing.

SERVICIOS

Informes y monitorización en tiempo real: Todas las soluciones empresariales de Optenet incluyen el sistema de informes y monitorización en tiempo real más rápido disponible. Los informes, respaldados por una base de datos que incorpora la solución sin necesidad de licencias adicionales, se pueden personalizar en función de las necesidades empresariales.

ADMINISTRACIÓN CENTRALIZADA POR CAPAS

Administración central y operaciones distribuidas: Mediante una potente y a la vez sencilla consola de gestión centralizada, la administración de políticas para varias ubicaciones y varias máquinas no implica ningún esfuerzo. Los administradores pueden usar la consola para definir y ejecutar políticas de bloqueo sin límite, aplicables en una escala global, independientemente de la infraestructura de la red.

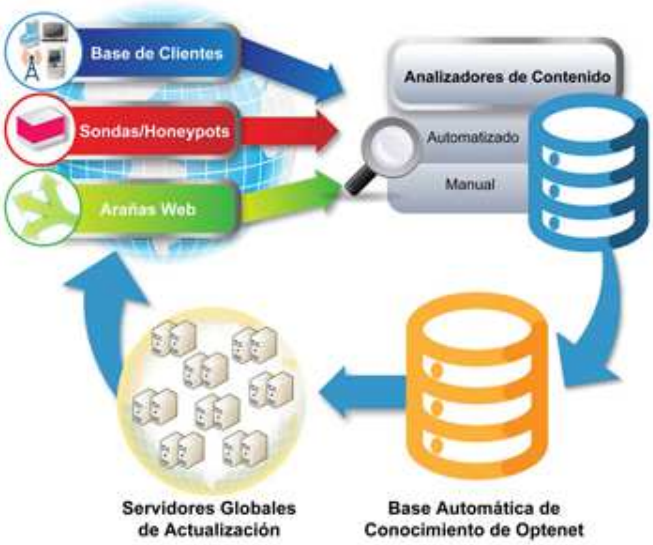
Administración por capas eficiente y efectiva: Los administradores pueden configurar de forma sencilla y efectiva y personalizar las políticas de acceso por usuario, grupo, estación de trabajo o red, ya sea de forma local o global. De esta forma, resulta sencillo permitir un nivel de acceso para todas las ubicaciones o proporcionar administración local con diferentes niveles de acceso, de acuerdo con necesidades específicas. El sistema de administración por capas proporciona una flexibilidad que permite a las empresas protegerse con la máxima granularidad y eficiencia.

TECNOLOGÍA DE CLASIFICACIÓN DINÁMICA DE CONTENIDO

Optenet MailSecure™ proporciona los niveles de precisión más altos a la hora de eliminar y gestionar las amenazas de correo entrante y saliente. El producto incorpora un sistema de detección de multicapa que combate el spam en diferentes niveles como: bases de datos de reputación, listas de direcciones sospechosas, análisis de URLs y verificación de firmas digitales.

Optenet GIANT™ recibe flujos de información constantes de fuentes de Internet en todo el mundo y actualiza cada instancia de la solución de Optenet, permitiendo que las nuevas amenazas se bloquean correctamente al poco de aparecer.

GIANT Global Intelligence Acquisition Network for Threats



Solución de mercado elegida

StoneGate de Stonesoft

Características

El sistema de prevención de intrusos (IPS) StoneGate protege la red interna mientras que el Firewall/VPN StoneGate proporciona protección del perímetro y conectividad segura entre oficinas remotas.

StoneGate IPS protege la red interna mientras que el Firewall/VPN StoneGate proporciona protección del perímetro y conectividad segura entre oficinas remotas.

Por las características y funcionalidades que proporciona se utilizará el modelo IPS-1030. Disponibles en *[14]*:

Licensed Performance	
Throughput	200 Mbps
Latency	< 150 microseconds
Concurrent connections	> 300 000
Connections/sec	> 15 000
SSL inspection for client/server	40 Mbps / 40 Mbps

Hardware

Network interfaces	
Ethernet	6 x 10/100/1000 copper
Bypass interface pairs	2
Connectors	RS-232 serial console, 2 x USB

Al igual que los cortafuegos, para realizar la gestión y el funcionamiento adecuado de los IPS, se necesita del SMC (StoneGate Management Server).

Desde el SMC se gestionarán todos los sensores IPS y los analizadores (Analyzer Server), que serán los encargados de correlar las secuencias de eventos en tiempo real que notifican los citados sensores.

El Analyzer es capaz de aislar un atacante o gusano en todos los nodos FW e IPS de forma simultánea, minimizando así el posible daño que se pueda causar en la red.

A continuación se muestra una captura de pantalla de lo que serían políticas de IPS:

IPS Sensor Policy

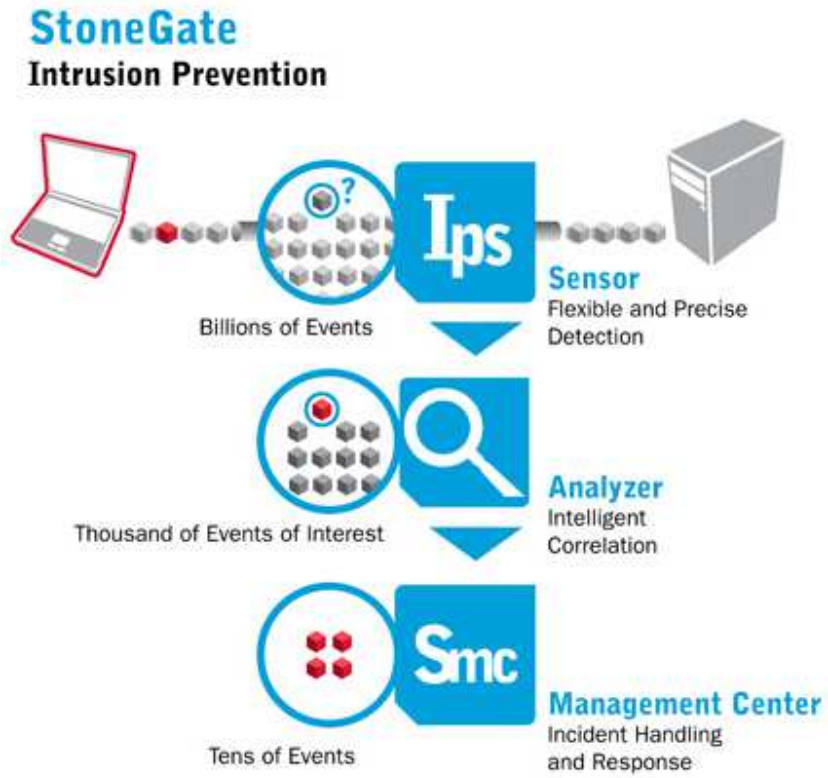
Ethernet Rules | Access Rules | IPv6 Access Rules | Inspection Rules

	ID	Situation	Logical ...	Source	Destination	Sev..
⊟	Prohibited Applications					
	1.13	Instant Messaging	ANY	ANY	ANY	ANY
	1.14	Peer to Peer	ANY	ANY	ANY	ANY
	1.15	Online Gaming Protocols	ANY	ANY	ANY	ANY
⊟	Possible Malicious Activity					
	1.17	Possibly Unwanted Content	ANY	ANY	ANY	ANY
	1.18	Suspicious traffic	ANY	ANY	ANY	ANY
	1.19	Potential Compromise	ANY	ANY	ANY	ANY
	1.20	Potential Disclosure	ANY	ANY	ANY	ANY
⊟	Confirmed Malicious Activity					
	1.22	Spyware, Malware and Adware	ANY	ANY	ANY	ANY
	1.23	Attacks	ANY	ANY	ANY	ANY
	1.24	Successful Attacks	ANY	ANY	ANY	ANY

Esto sería una captura de pantalla de log de IPS:

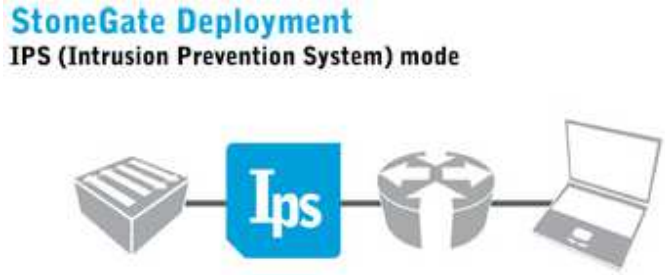
HTTP_CSH-Firefox-3.5.0-Browser-Usage	Info	HTTP	77.79.86.43
HTTP_CSH-Firefox-3.5.1-Browser-Usage	Info	HTTP	77.79.86.43
HTTP_CSH-Firefox-Browser-Usage	Low	HTTP	77.79.86.43
HTTP_SLS-Successful-Status-Code	Info	HTTP	77.79.86.43
MSSQL_MS-SQL-Server-Resolution-Service...	Critical	MSSQL (UDP)	61.138.78.23
MSSQL_MS-SQL-Slammer-Worm-Propagati...	High	MSSQL (UDP)	61.138.78.23
HTTP_Request-GET	Info	HTTP	67.237.116.172
HTTP_Request-Version-1.1	Info	HTTP	67.237.116.172
HTTP_CSH-Googlebot-Web-Spider	Low	HTTP	67.237.116.172
HTTP_SLS-Successful-Status-Code	Info	HTTP	67.237.116.172
Ethernet_Frame-Discarded	Info	CDP	
DNS_Standard-Query-Reply-Failure	Info	DNS (UDP)	78.62.147.54
DNS_Standard-Query-Reply-Failure	Info	DNS (UDP)	78.62.147.54
SMTP_Whitespace-Extra	Low	SMTP	154.48.234.160

La estructura del funcionamiento es la siguiente *[14]*:

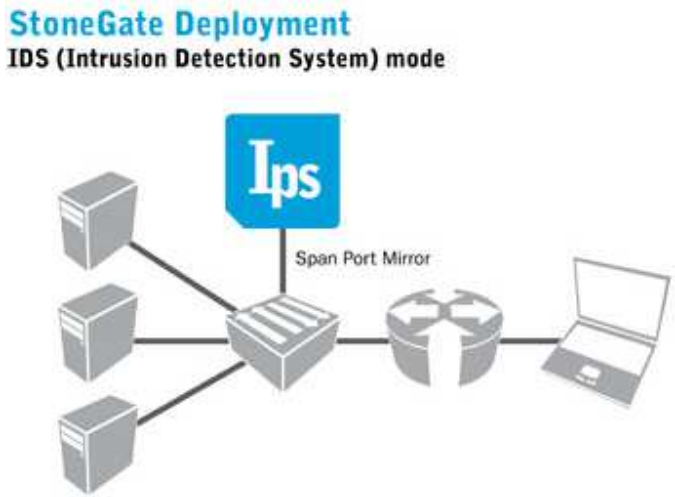


Son tres las formas en las que se puede desplegar este IPS (al igual que todos los demás):

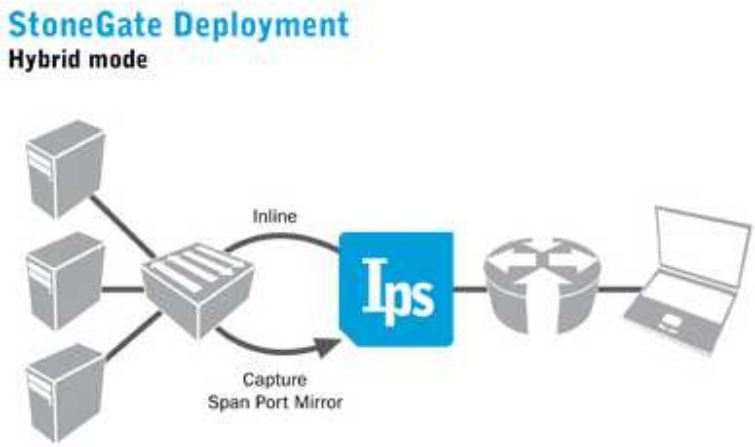
1. Modo IPS (Intrusion Prevention System), opción en la que el IPS podrá cortar posibles ataques que sucedan en la red.



2. Modo IDS (Intrusion Detection System), donde el sensor solo notificará los posibles ataques, sin tener la posibilidad de cortarlos.



3. Modo híbrido, que será una mezcla de ambas configuraciones anteriores.



En el escenario recreado se aplicará la implementación en modo IPS.

El IPS de StoneGate proporciona una ***protección*** contra la entrada ilegal de tráfico y ***contra los ataques de denegación de servicio*** sin perturbar el tráfico legítimo de la red.

StoneGate utiliza unas técnicas de correlación únicas en la detección de patrones de comportamiento sospechosos en la comunicación de servicios Web. Una vez que StoneGate ha detectado el host atacante, bloqueará la comunicación de éste hacia el servidor interno de la red donde se aloja el servicio Web.

También será capaz de realizar ***filtrado de URLs***, ya que posee una base de datos con millones de web categorizadas, posibilitando al administrador el tener unas listas blancas y negras para realizar la mejor política de seguridad posible.

Es capaz de ***inspeccionar tráfico SSL***, proporcionando a los administradores de red la capacidad de monitorizar el tráfico TLS / SSL para detectar y reaccionar a cualquier contenido no deseado.

Alternativas

ISS de IBM

Internet Security System RealSecure Server Sensor es una herramienta distribuida de detección de intrusos en tiempo real que proporciona soluciones de IDS en plataforma final (HIDS). Para ello monitoriza en tiempo real la actividad desarrollada por el servidor (llamadas a sistema operativo, logs, accesos de usuarios, actividad de red) en busca de patrones susceptibles de ser considerados violaciones de seguridad. La plataforma RealSecure se basa en un modelo clásico de detección de ataques por localización de patrones.

El conjunto de actividades monitorizadas por RealSecure son respaldadas por una base de datos que incluye cerca de 6500 patrones de ataques, continuamente actualizada por el servicio ISS X-Force. Esta base de datos de patrones responde a violaciones de seguridad de distinta naturaleza:

- Escaneos y exploraciones.
- Ataques de denegación de servicio.
- Exploits
- Backdoors y troyanos.
- Ataques específicos de sistemas (Windows, Unix, Novel, etc.)
- Intentos de acceso no autorizado
- Actividades sospechosas

Las principales características de RealSecure que lo convierten en un candidato ideal para el presente proyecto son las siguientes *[18]*:

- Incrementa el nivel de seguridad: La monitorización de la actividad en los servidores, así como la búsqueda de actividades maliciosas y el envío de alarmas, permite incrementar la seguridad de la infraestructura de acceso a Internet.

- Gestión: La interfaces de gestión del sistema de intrusos son muy intuitivas. Esto facilitará la gestión a los administradores que no estén familiarizados con este tipo de tecnologías y mejorará considerablemente la seguridad al evitar fallos en las configuraciones de seguridad.

- Sistema de notificación: Es posible definir distintos mecanismos de alarma y notificación de eventos, comprendiendo alarmas de consola, notificación mediante correo electrónico, envío de traps SNMP, etc.

- Generación de informes: Incorpora un elevado número de informes predefinidos, permitiendo que los mismos sean personalizados y adaptados para los distintos niveles jerárquicos de la organización.

- Gestión de actualizaciones: Mediante el servicio X-Force, se dispone de actualizaciones periódicas de los patrones de ataque que pueden ser distribuidas a las distintas sondas desde la consola centralizada.

- Gestión centralizada: Toda la gestión, administración y monitorización del sistema de detección de intrusos se realiza mediante la consola RealSecure SiteProtector. Desde la consola se establecen conexiones cifradas con cada sonda gestionada.

Respuesta automatizada a eventos: Es posible definir acciones automáticas ante eventos de seguridad: registro del evento, grabación de sesiones para análisis forense, terminación de conexiones, bloqueo de conexiones, bloqueo de cuentas, reconfiguración automática de las políticas de cortafuegos, etc…lo cual permite definir políticas de respuesta temprana ante violaciones de seguridad.

RealSecure SiteProtector es la solución para gestionar de forma centralizada los IDS de host distribuidos en los servidores de la organización. Esta solución también proporciona escalabilidad (puede gestionar varios cientos de IDS) y análisis de la información recibida. Todo esto, además de mejorar la seguridad considerablemente, reduce el coste de gestión mediante la consola única de gestión que se comunica transparentemente con la base de datos donde almacena toda la información recibida y facilita tanto las tareas administrativas como las de mantenimiento y soporte.

Otra característica de RealSecure SiteProtector es la posibilidad de crear carpetas donde se agrupan los sensores en función de las necesidades de los administradores: agrupación geográfica, topológica, política, etc. Esto proporciona flexibilidad, adaptabilidad de la solución a cualquier entorno y facilidad de manejo.

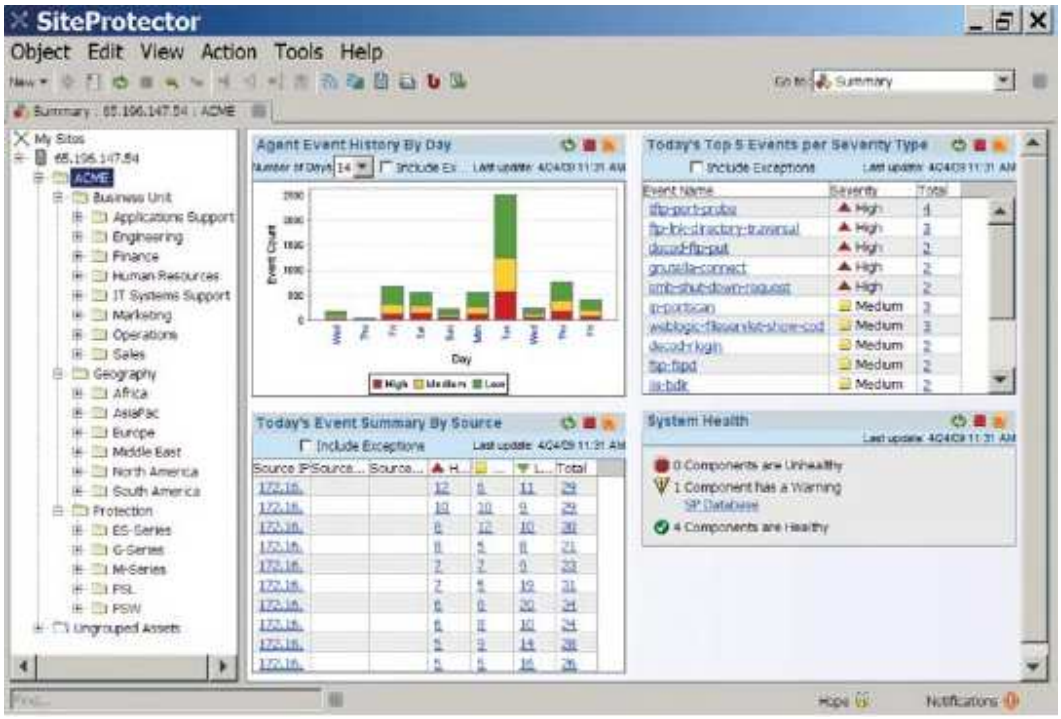
La monitorización de actividades sospechosas y el envío de alertas frente a incidentes están centralizados en SiteProtector. Los sensores envían la información y, dependiendo de la configuración de la política de seguridad implementada, SP enviará las alertas pertinentes para combatir eficientemente

cualquier ataque a los sistemas de información. En este punto, la labor de SIS es fundamental porque un ajuste incorrecto de la solución proporcionará demasiada información inútil que confundirá a los administradores de la solución y no servirá para mucho. Por ello, es necesario un conocimiento avanzado en el campo de la seguridad de la información y de la propia solución.

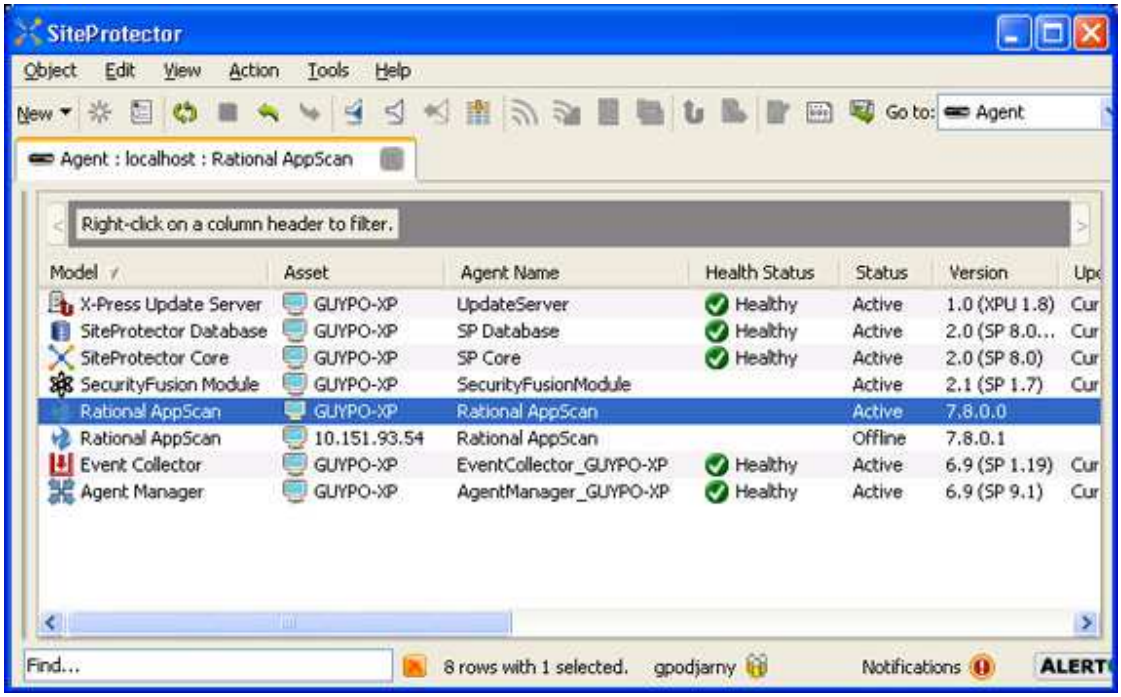
Otra de las mayores preocupaciones de los administradores de seguridad es la actualización de los dispositivos. SP ofrece una actualización automatizada de productos mediante X-Press Update (incluido con SP) que reduce la actualización de las firmas de detección a un simple clic de ratón. Esta facilidad de actualización mejora la seguridad porque nuestros equipos estarán actualizados con una gestión administrativa mínima.

A continuación se muestran unas capturas de pantalla de la aplicación de SiteProtector:

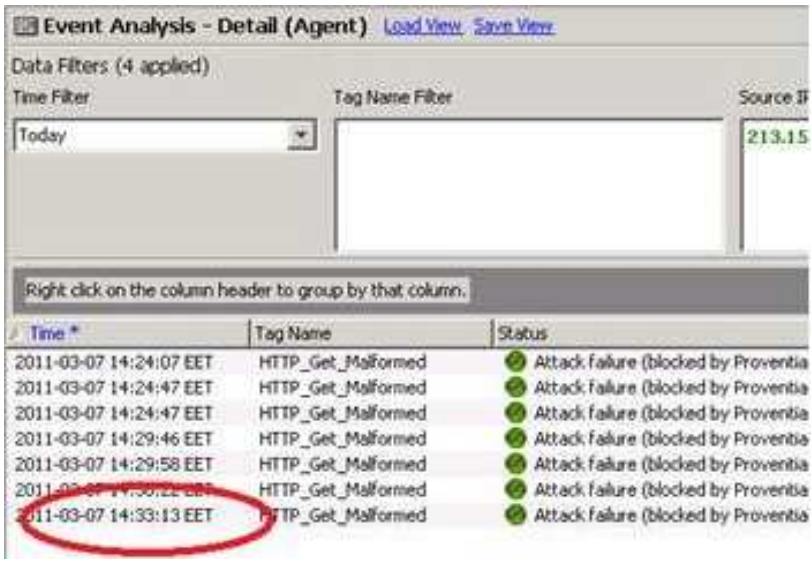
- Pantalla de Resumen:



- Pantalla de agentes desplegados:



- Pantalla de logs:



Esta solución se implantará sobre un servidor HP DL 120 G7, ya que por especificaciones técnicas cumple con los requisitos necesarios para el servicio.

A continuación se muestran las principales características del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Core™ i3 2100 (2 núcleos, 3,1 GHz, 3 MB, 65 W, 1333/t)
Número de procesadores	1
Núcleo de procesador disponible	2
Memoria, estándar	2 GB
Ranuras de memoria	4 ranuras DIMM
Tipo de memoria	PC3-10600E DDR3 UDIMMs
Ranuras de expansión	2
Controlador de red	(2) 1 puerto NC112i 1 GbE
Tipo de fuente de alimentación	(1) detección automática de 400 W, cumple con la marca CE
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	Ningún estándar de suministro
Formato (totalmente configurado)	1U
Garantía - año(s) (partes/mano de obra/in situ)	1/1/1

Solución de mercado elegida

SW Libre en Linux (BIND)

Características

Según se indica en *[19]*, "BIND (*Berkeley Internet Name Domain*), como implementación del protocolo DNS, es el servidor de este tipo más comúnmente usado en internet. La necesidad administrativa de montar un servidor de nombres DNS hacen de BIND una de las primeras opciones a tener en cuenta.

BIND es uno de los primeros servidores DNS creados al albor de internet. Encargado y patrocinado por la DARPA (*Defense Advanced Research Projects Agency*) a principios de los años ochenta, cuando el Departamento de Defensa estadounidense estaba implicado en el desarrollo de la red de redes, el proyecto queda finalmente en manos de DEC/Digital (*Digital Equipment Corporation*), que se encarga de desarrollarlo casi por completo. Finalmente es uno de los empleados de Digital, Paul Vixie, quien retomará el proyecto y lo incluirá en el consorcio ISC (*Internet Software Consortium*), responsable actual del mantenimiento del programa.

Si bien las primeras implementaciones del servidor BIND (en concreto las versiones 4 y 8) mostraban una cantidad de vulnerabilidades exagerada (como casi todo el software nacido a la par que internet), la versión 9 del producto ya no presenta tantas complicaciones. Escrita desde cero para superar las dificultades técnicas de antiguos desarrollos, dicha versión fue impulsada por proveedores UNIX, deseosos de que BIND mantuviera la competencia con Microsoft en igualdad de condiciones y por el Ejército de los Estados Unidos, que desarrolló funcionalidades relativas a la seguridad como DNSSEC (*DNS*

Security Extensions), al darse cuenta de que la seguridad dentro del servicio DNS es algo a tener muy en cuenta.

Características de BIND

BIND 9 ofrece un servidor de nombres de dominio a través de named, una biblioteca de resolución de sistemas de nombres de dominio y un paquete de herramientas para monitorizar el correcto funcionamiento de todo el sistema (bind-utils).

Entre sus principales características se incluyen los protocolos de seguridad como DNSSEC o TSIG (Transaction SIGnature) y el soporte de IPv6, nsupdate (actualizaciones dinámicas), notificación DNS, rndc flush, vistas y procesamiento en paralelo. Gracias a su arquitectura mejorada se ha conseguido una mejor portabilidad entre sistemas."

El servicio de DNS que se configurará en la DMZ se encargará de atender las peticiones de nombres de equipos accesibles desde Internet que están alojados en esta red.

Se realizará una configuración de forma que uno de los servidores sea el servidor primario y el otro el servidor secundario; el secundario se sincronizará (de acuerdo con la propia definición del protocolo de DNS) con el servidor primario para mantener en todo momento una información consistente en ambos servidores.

Conceptos de DNS y configuraciones que se pueden encontrar en *[19]*:
Configuración

Antes de comenzar con los ficheros de configuración del programa, es preciso tener claros los datos siguientes:

- Nombre de dominio a resolver.

- Servidor de nombres principal (DNS Maestro/SOA). Dicho nombre tiene que estar plenamente resuelto y, por supuesto, tiene que ser FQDN.

- Lista de servidores de nombres (NS) para la redundancia. Igual que en el caso anterior, deberán estar plenamente resueltos y ser FQDN.

- Cuenta de correo del administrador de la zona. Cuenta real y distinta de la zona a resolver.

- Servidor de correo (MX) con registro A (no vale un CNAME).

- IP predeterminada del dominio.

- Subdominios y direcciones IP asociadas a los mismos (www, mail, ftp,...).

En resumen, la configuración de un DNS con BIND se basa en tres tipos de ficheros:

Ficheros de zona:

Un fichero de zonas tiene, en principio, el siguiente aspecto:

```
$TTL 43200
@ IN SOA server.mydomain.name. user.server.mydomain.name.
(
200583909; Número de serie
3600 ; Tiempo de refresco (1 hora)
300 ; Tiempo entre reintentos de consulta (5 min)
17200 ; Tiempo de expiración de zona (2 days)
```

```
43200 ) ; Tiempo total de vida (TTL) (12 hours)
;
@ IN NS server.mydomain.name.

pc1 IN A xxx.xxx.xxx.xxx
pc2 IN A yyy.yyy.yyy.yyy

nombre1 IN CNAME pc1
nombre2 IN CNAME pc2
```

Los nombres de dominio terminan en un punto para indicar que son nombres absolutos.

Los distintos ficheros de zonas se encuentran, en una distribución tipo Red-Hat / Fedora en la rama /var/named (o /var/named/chroot/var/named). A continuación vamos a ver un fichero de zona para la configuración típica de un dominio:

```
$TTL 86400
@ IN SOA dominio_ejemplo.org. postmaster.dominio_ejemplo.org. (
42 ; serial
3H ; refresh
15M ; retry
1W ; expiry
1D ) ; minimum
@ IN NS ns1.dominio_ejemplo.org.
@ IN NS ns2.dominio_ejemplo.org.
@ IN MX 10 mx1.dominio_ejemplo.org.
@ IN MX 20 mx2.dominio_ejemplo.org.
@ IN TXT "dominio_ejemplo.org"
@ IN HINFO "Intel Pentium IV" "Fedora Core"
```

```
@ IN A 215.127.55.12
ns1 IN A 214.125.33.41
ns2 IN A 215.127.55.12
mx1 IN A 215.127.55.12
mx2 IN A 214.125.33.41
www IN A 215.127.55.12
www2 IN A 215.127.55.12
webmail IN A 215.127.55.12
smtp IN A 215.127.55.12
redirect IN CNAME dominio_ejemplo.no-ip.info

smtp.tcp SRV 0 0 25 mx1.dominio_ejemplo.org.
http.tcp SRV 0 3 80 dominio_ejemplo.org.
http.tcp SRV 0 1 80 www2.dominio_ejemplo.org.
https.tcp SRV 1 0 443 dominio_ejemplo.org.
pop3s.tcp SRV 0 0 995 mx1.dominio_ejemplo.org.

*.tcp SRV 0 0 0 .
*.udp SRV 0 0 0 .
```

Cada uno de los significados de cada parámetro ya se explicó en el punto de "Descripción de elementos de seguridad", por lo que no se explicarán en este punto.

Traducción inversa:

Es requerido en un servidor DNS que las direcciones IP se conviertan igualmente en nombres (***reverse lookup***). Dicha traducción se usará por parte de diferentes servidores y es muy aconsejable tener definida una zona de este tipo en un servidor DNS. Para la resolución inversa usaremos el pseudo-dominio in-addr.arpa. Quedando la dirección pública 55.127.215.in-addr.arpa.

(la parte de red de la dirección IP escrita al revés más el dominio). Un fichero de zona de resolución inversa para el dominio anterior quedaría como sigue:

```
$TTL 604800
@ IN SOA dominio_ejemplo.org. postmaster.dominio_ejemplo.org. (
42 ; serial
3H ; refresh
15M ; retry
1W ; expiry
1D ) ; minimum
@ IN NS ns1.dominio_ejemplo.org.
NS ns2.dominio_ejemplo.org.
12 IN PTR ns1.dominio_ejemplo.org.
```

Para la zona inversa de localhost podríamos generar un fichero parecido al siguiente:

```
$TTL 604800
@ IN SOA localhost. postmaster.dominio_ejemplo.org. (
42 ; serial
3H ; refresh
15M ; retry
1W ; expiry
1D ) ; minimum
IN NS ns1.dominio_ejemplo.org.
1 IN PTR localhost.ns1.dominio_ejemplo.org.
```

Hay que tener en cuenta que la zona de resolución inversa del dominio sólo funcionará en el caso de que ésta quede delegada convenientemente por el proveedor de servicios que se ocupa del rango de direcciones. Si es imprescindible, y el autor de este artículo considera que siempre debería serlo, tener una zona de resolución inversa para nuestra dirección o rango de

direcciones, será imperativo contactar con el proveedor de servicios para que dé de alta un registro NS para la zona en concreto.

Fichero named.conf:

El archivo named.conf se sitúa en la rama /etc o /etc/bind y estructura toda la información de zonas del servidor DNS. A grandes rasgos, podemos dividir el fichero en tres secciones: options, que define opciones de configuración general, loggin, que especifica la salida de la información y zone, donde se incorporan los datos generales de los archivos de zonas que ya hemos explicado en los puntos anteriores.

- Options:

  Habitualmente, las opciones incluidas por defecto en los ficheros de configuración de cada distribución para el apartado options son más que suficientes para arrancar el servidor DNS sin ningún tipo de problema. Dichas opciones son demasiado extensas para explicarlas en este artículo, así que es muy recomendable acceder a la página del manual referente a named.conf y leer para qué sirve cada opción y si alguna de ellas puede servir a nuestros propósitos. Una opción importante a tener en cuenta es la de fordwarders, que se usará para suministrar al servidor DNS las direcciones IP de los redireccionadores encargados de consultar ciertas direcciones a otros servidores DNS, cuando éstas no estén disponibles de forma local. De usarse el apartado, deberá quedar como el ejemplo siguiente:

```
    forwarders {
200.33.146.209;
200.33.146.217;
};
```

- Zone:

Bajo la definición de zone se darán de alta todas las zonas para nuestros dominios. Habrá que definir siempre una primera zona raíz (un punto), que informará de todos los servidores raíz a nuestro servidor DNS, y seguidamente se darán de alta todas y cada una de las zonas necesarias para el funcionamiento correcto de nuestro servidor. La zona raíz quedará como sigue (el fichero de zona puede conseguirse en la dirección ftp.internic.net/domain/named.cache):

```
    zone "." {
type hint;
file "named.ca";
};
```

Un ejemplo de definición de zona general podría ser el siguiente:

```
    zone "dominio_ejemplo.org" {
type master;
file "/var/named/dominio_ejemplo.org.zone";
allow-query { any; };
allow-transfer { slaves; };
};
```

Con type master se establece el servidor como maestro/primario (slave establecerá el tipo secundario). file indica la ruta de acceso al fichero de configuración de la zona declarada. allow-query { any; } especifica que es posible hacer consultas externas a la zona. allow-transfer { slaves; } transfiere la configuración de la zona hacia los servidores secundarios especificados en el ACL slaves dentro del fichero de configuración de la forma siguiente:

```
    acl "slaves" {
215.66.73.59;
};
```

- *Logging:*

Bajo la sentencia logging se definen los canales y archivos hacia donde se dirigirán los mensajes de auditoría de BIND. Una sentencia logging se construye de la forma siguiente:

```
    logging {
definición_de_canal;
definición_de_canal;
...
category nombre_categoría {
nombre_canal;
nombre_canal;
...
};
};
```

A continuación ponemos un ejemplo de logging para establecer los mensajes de aviso y las consultas al servidor y redirigirlos hacia distintos ficheros de texto:

```
    logging {

channel warning
{
file "/var/log/server-dns/warning" versions 3 size 100k;
```

```
severity warning;
print-category yes;
print-severity yes;
print-time yes;
};

channel general_dns
{
file "/var/log/server-dns/log" versions 3 size 100k;
severity info;
print-category yes;
print-severity yes;
print-time yes;
};
category default { warning; } ;
category queries { general_dns; } ;
    };
```

La implantación del servicio de DNS se va a llevar a cabo sobre dos servidores HP ML 330 G6, ya que son servidores más potentes, con más memoria (4GB) y un procesador de 4 núcleos. Además dispone de dos tarjetas de red que serán las que se utilicen, ampliables con más ranuras.

A continuación se muestran las características más importantes del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Xeon® E5606 (4 núcleos, 2,13 GHz, 12 MB L3, 80 W)
Número de procesadores	1
Núcleo de procesador disponible	4
Memoria, estándar	4 GB
Ranuras de memoria	12 ranuras DIMM
Tipo de memoria	PC3-10600E (UDIMM)
Ranuras de expansión	(4) ranuras PCI-E y (2) ranuras PCI-X opcionales, con ampliador PCI X (usa 1 ranura PCI-E)
Controlador de red	(1) 2 Puertos 1 GbE NC326i
Descripción de unidad	(8) SAS/SATA LFF; sin conexión en caliente o conexión en caliente
Tipo de fuente de alimentación	(1) 460 W sin conexión en caliente, no redundante
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	DVD-ROM SATA media altura
Formato (totalmente configurado)	Bastidor de 5U, torre
Garantía - año(s) (partes/mano de obra/in situ)	3/1/1

Alternativas

DNS de Microsoft

Para instalar un servidor DNS de Microsoft, bastará con instalar un sistema operativo Microsoft Windows NT (en el mismo servidor que se utiliza para la instalación de un DNS sobre software libre), y a partir de ahí utilizar el servicio de DNS de dicho sistema.

Más detalladamente se haría de la siguiente manera, tal y como se puede ver en *[20]*:

1. Haga clic en el botón Inicio, seleccione Configuración y, a continuación, haga clic en panel de control. Haga doble clic en el icono red y, a continuación, haga clic en la ficha Servicios.
2. Haga clic en Agregar, seleccione Microsoft DNS Server desde la red Seleccionar servicio de cuadro de diálogo y, a continuación, haga clic en Aceptar.
3. Escriba la ubicación de los archivos de origen de Windows NT, haga clic en Aceptar y, a continuación, haga clic en Cerrar.

   Nota: si tiene cualquier service Pack instalado, deberá volver a aplicar el service pack antes de reiniciar el equipo.

4. Reinicie el equipo.

Para crear el servidor DNS se hará de la siguiente forma:

1. Haga clic en el botón Inicio, seleccione Programas, herramientas administrativas y, a continuación, haga clic en Administrador de DNS.
2. En el menú DNS, haga clic en nuevo servidor.
3. Escriba la dirección IP del servidor DNS en el cuadro de diálogo Agregar servidor de DNS cuadro y, a continuación, haga clic en Aceptar.

Nota: no es necesario reiniciar el servidor DNS para los cambios en las zonas surta efecto. Todo lo que necesita es para que los archivos de datos de servidor para actualizarse en el paso siguiente:

- En el Administrador de DNS, haga clic con el botón secundario en el servidor DNS y haga clic en Actualizar servidor archivos de datos.

Crear la zona de búsqueda inversa:

Algunas aplicaciones utilizan una consulta inversa a un servidor DNS para buscar el nombre de host de un host cuando tiene la dirección IP del equipo. Debe configurar una zona de búsqueda inversa para proporcionar esta capacidad.

Nota: las zonas de búsqueda inversa no pueden ser necesarias en la red pero se recomienda que uno esté presente. NSLOOKUP se ejecutan en el servidor DNS fallará si no se configura ninguna zona de búsqueda inversa.

Para crear una zona de búsqueda inversa, siga los pasos siguientes:

1. En el Administrador de DNS, haga clic con el botón secundario en el servidor DNS y, a continuación, haga clic en zona nueva.
2. Haga clic en principal en el cuadro de diálogo "Crear nueva zona para" y, a continuación, haga clic en Siguiente.
3. El nombre de zona se deriva de la dirección de red. En la información del ejemplo, el nombre de zona es 58.168.192.in-addr.arpa. Escriba su nombre de zona inversa (la parte menos significativa de la dirección IP y el trabajo hacia la parte más importante de la dirección). Por ejemplo:

If your network ID is:	Then your reverse zone is:
10.0.0.0	10.in-addr.arpa
130.20.0.0	20.130.in-addr.arpa
250.30.203.0	203.30.250.in-addr.arpa

Nota: la sintaxis de la zona de búsqueda inversa es imprescindible para su funcionamiento.

3. Después de escribir el nombre de zona de búsqueda inversa, presione TAB y el inverso nombre de archivo de zona de búsqueda se rellene automáticamente utilizando el nombre de zona en el paso 3 anexada ".dns" (sin las comillas).
4. Haga clic en siguiente y, a continuación, haga clic en Finalizar.

Crear la zona de búsqueda directa:

1. En el Administrador de DNS, haga clic con el botón secundario en el servidor y, a continuación, haga clic en zona nueva.
2. Haga clic en zona principal y, a continuación, haga clic en Siguiente.
3. Escriba el nombre de zona para su dominio DNS. Éste es el nombre de dominio que está registrado con InterNIC (<Domain.com> en el ejemplo).
4. Presione la tecla TAB, haga clic en siguiente y, a continuación, haga clic en Finalizar.

Cuando haya creado la zona de búsqueda directa, debe ver tres registros crean automáticamente en esa zona: el registro NS, el registro SOA y un registro. Si no tienen los tres de estos, quizás desee comprobar que la configuración de DNS en las propiedades de TCP/IP está configurada correctamente (haga clic

en el botón Inicio, seleccione Configuración, haga clic en Panel de control y, a continuación, haga doble clic en el icono red).

Nota: sólo se creará el registro si el nombre de zona coincide con el nombre de dominio.

Agregar registros de host a la zona de búsqueda directa:

El registro para el servidor DNS debería haberse creado automáticamente. Sin embargo, el Administrador de DNS no crea automáticamente el registro PTR en la zona inversa para el servidor DNS. El más sencillo para corregir este problema consiste en utilizar los siguientes pasos:

1. Haga clic con el botón secundario en el registro para el servidor DNS y, a continuación, haga clic en Eliminar registro.
2. Haga clic en Sí en el cuadro de diálogo de confirmación.
3. Haga clic con el botón secundario en su avance zona <Domain.com> y a continuación, haga clic en nuevo host.
4. Escriba el nombre de host del servidor DNS y la dirección IP.
5. Haga clic en Crear registro PTR asociado para habilitar y haga clic en Agregar Host.
6. Haga clic en Listo.

Nota: Repita los pasos 3 a 5 anteriores para todos los servidores desea agregar a su dominio DNS.

Para comprobar que los registros PTR se crean correctamente, haga clic con el botón secundario en el 58.168.192.in-addr.arpa de zona de búsqueda inversa y, a continuación, haga clic en actualizar.

Configurar otros tipos de registro

Un servidor DNS puede ser responsable de varios tipos de registro diferente. Algunas de ellas incluyen, pero no están limitados a la siguiente: A, CNAME,

HINFO, MX, NS y SOA. Para obtener detalles sobre estos y otros tipos de registro, consulte las notas DNS que se ha mencionado anteriormente en este artículo.

Crear un registro CNAME:

Un registro CNAME le permite utilizar varios nombres para la misma dirección IP. De esta forma, puede hacer que los usuarios acceso al mismo servidor para funciones independientes, como FTP1.domain.com WWW.domain.com. Antes de poder crear el registro CNAME, primero debe tener un registro, como se describió anteriormente.

Para crear un registro CNAME, siga los pasos siguientes:

1. Haga clic con el botón secundario en su avance la zona, <Domain.com> y haga clic en nuevo registro.
2. Seleccione registro CNAME del cuadro de lista Tipo de registro en el nuevo recurso de cuadro de diálogo Grabar.
3. Escriba un nombre alternativo para tener acceso a este equipo. Por ejemplo, en la información de ejemplo anteriormente en este artículo, WWW es un nombre alternativo para FTP1.domain.com.
4. Escriba el nombre host original en "De host DNS Name". Por ejemplo, <FTP1.domain.com>.

   Nota: es importante utilizar el nombre de dominio completo (FQDN) para el nombre DNS de host original.

5. Haga clic en Aceptar.

Ahora cuando los usuarios crear una consulta para cualquiera de estos nombres de host, el servidor DNS devolverá la misma dirección IP.

Crear un registro MX:

Un registro MX es un registro de correo Exchange que señala los programas de correo a los servidores de correo. Para crear un registro MX, siga los pasos siguientes:

1. Haga clic con el botón secundario en la búsqueda hacia adelante zona <Domain.com> y, a continuación, haga clic en nuevo registro.
2. Seleccione registro MX del cuadro de lista Tipo de registro en el nuevo recurso de cuadro de diálogo Grabar.
3. El campo nombre de host (opcional) se utiliza para el nombre de host del servidor de correo. Sin embargo, si desea que los usuarios puedan enviar correo a su dominio utilizando el formato USER@Domain.com, deje el campo nombre de host en blanco.

Nota: si el registro MX contiene el nombre de host, enviar correo a usuario@dominio.com no funcionen. Hay tres formas de resolver este problema. En primer lugar, elimine el nombre de host del registro MX como se describe en el paso 3. En segundo lugar, una vez creado el registro MX con el nombre de host, crear un registro "A" para el dominio que no tenga ningún nombre de host. En tercer lugar, elimine el registro MX existente y volver a crear como se describe en los pasos del uno al seis en la creación una sección de registro MX de este artículo.

4. Escriba el FQDN del servidor de correo en el nombre DNS de correo Exchange Server, por ejemplo, Mail.domain.com.

Nota: hay un punto final ".", tras el DNS de servidor de correo Exchange nombre. El FQDN que se utiliza para el servidor de correo de Exchange debe tener un registro para ese dominio correspondiente. Si el servidor de correo de Exchange es un equipo diferente que el servidor DNS, el servidor DNS debe saber dónde redirigir el tráfico de correo.

5. El número de preferencia es cualquier número de 0 a 65535. En el caso de varios servidores de correo, este número identifica qué correo servidor va a utilizarse por primera vez. Cuanto menor sea la preferencia de número, cuanto mayor sea la prioridad.
6. Haga clic en Aceptar.

Para crear una delegación de zona

1. Abra DNS.
2. En el árbol de la consola, haga clic con el botón secundario del ***mouse*** (ratón) en el subdominio correspondiente y, a continuación, haga clic en **Delegación nueva**.
3. Siga las instrucciones proporcionadas por el Asistente para agregar nueva delegación con el objeto de terminar la creación de un nuevo dominio delegado.

Notas

- Para llevar a cabo este procedimiento, debe ser miembro del grupo Administradores en el equipo local o tener delegada la autoridad correspondiente. Si el equipo está unido a un dominio, los miembros del grupo Administradores de dominio podrían llevar a cabo este procedimiento. Como práctica recomendada de seguridad, considere la posibilidad de utilizar la opción Ejecutar como para llevar a cabo este procedimiento.

- Para abrir DNS, haga clic en **Inicio**, **Panel de control**, haga doble clic en **Herramientas administrativas** y, a continuación, haga doble clic en **DNS**.

- Todos los dominios o subdominios que aparecen como parte de la delegación de zona aplicable se deben crear en la zona actual antes de realizar la delegación como se describe aquí. Según sea necesario, utilice la consola de DNS para agregar dominios a la zona antes de

terminar este procedimiento. Para obtener más información, vea delegar zonas.

Para proteger un servidor DNS

1. Abra DNS.
2. En el árbol de la consola, haga clic con el botón secundario del ***mouse*** (ratón) en el servidor DNS correspondiente y, a continuación, haga clic en **Propiedades**.
3. En la ficha **Interfaces**, asegúrese de que el servidor DNS escucha las interfaces correctas.
4. En la ficha **Opciones avanzadas**, active la casilla de verificación **Asegurar caché contra corrupción**.
5. Si el servidor DNS no va a realizar resoluciones recursivas, active la casilla de verificación **Deshabilitar recursividad**.

Notas

- Para llevar a cabo este procedimiento, debe ser miembro del grupo Administradores en el equipo local o tener delegada la autoridad correspondiente. Si el equipo está unido a un dominio, los miembros del grupo Administradores de dominio podrían llevar a cabo este procedimiento. Como práctica recomendada de seguridad, considere la posibilidad de utilizar la opción Ejecutar como para llevar a cabo este procedimiento.

- Para abrir DNS, haga clic en Inicio, Panel de control, haga doble clic en Herramientas administrativas y, a continuación, haga doble clic en DNS.

Si hay una zona DNS almacenada en Active Directory, también puede proteger esa zona DNS y sus registros de recursos mediante las características de seguridad de Active Directory.

- De manera predeterminada, una zona DNS sólo está autorizada para permitir transferencias de zona desde servidores DNS incluidos en las propiedades de la zona DNS.

- De forma predeterminada, el servicio DNS escucha las comunicaciones de mensajes DNS en todas las direcciones IP configuradas para el equipo servidor.

- Las direcciones IP de servidor que se agreguen aquí se tienen que administrar estáticamente. Si posteriormente cambia o quita direcciones especificadas aquí de las configuraciones TCP/IP que se mantienen en este servidor, actualice esta lista en consecuencia.

- La casilla de verificación Asegurar caché contra corrupción está activada de forma predeterminada.

- Si deshabilita la recursividad en este servidor DNS, no podrá utilizarlo para responder a consultas recursivas de clientes DNS ni establecer este servidor DNS como servidor de reenvío DNS. Deshabilite la recursividad en servidores DNS que sólo realicen iteraciones con otros servidores DNS.

- Al deshabilitar la resolución recursiva en este servidor DNS, puede evitar un ataque de denegación de servicio (DoS, Denial of Service) en el que un usuario malintencionado intente que este servidor DNS responda a consultas recursivas de un dominio ubicado en una zona DNS controlada por dicho usuario.

Solución de mercado elegida

SW libre en linux

Características

Adicionalmente en los servidores DNS se podrá instalar el servicio de NTP que servirá de servidor para todos los sistemas de la red corporativa.

Ya que se ha instalado el servidor DNS sobre Red Hat, se debe descargar el paquete (.rpm) para éste sistema operativo también.

Una vez descargado solo habría que instalarlo mediante el comando "yum install ntp-4.2.6p5-1.el5.pp.i386.rpm".

Una vez instalado el paquete de ntp, solo quedaría configurar el fichero ntp.conf para que el servidor se sincronice con otros servidores ntp oficiales.

Un ejemplo de configuración sería el que podemos encontrar en *[21]*:

```
# Se establece la política predeterminada para cualquier
# servidor de tiempo utilizado: se permite la sincronización
# de tiempo con las fuentes, pero sin permitir a la fuente
# consultar (noquery), ni modificar el servicio en el
# sistema (nomodify) y declinando proveer mensajes de
# registro (notrap).
restrict default nomodify notrap noquery

# Permitir todo el acceso a la interfaz de retorno del
# sistema.
```

restrict 127.0.0.1

Se le permite a la red local sincronizar con el servidor
pero sin permitirles modificar la configuración del
sistema, y sin usar a éstos como iguales para sincronizar.
restrict 192.168.0.0 mask 255.255.0.0 nomodify notrap

Reloj local indisciplinado.
Este es un controlador emulado que se utiliza solo como
respaldo cuando ninguna de las fuentes reales están
disponibles.
fudge 127.127.1.0 stratum 10
server 127.127.1.0

Fichero de variaciones.
driftfile /var/lib/ntp/drift
broadcastdelay 0.008

Fichero de claves si acaso fuesen necesarias para realizar
consultas
keys /etc/ntp/keys

Lista de servidores de tiempo de estrato 1 o 2.
Se recomienda tener al menos 3 servidores listados.
server 0.pool.ntp.org
server 1.pool.ntp.org
server 2.pool.ntp.org

Permisos que se asignarán para cada servidor de tiempo.
En los ejemplos, no se permite a las fuente consultar, ni
modificar el servicio en el sistema ni enviar mensaje de
registro.

restrict 0.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery

restrict 1.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery

restrict 2.pool.ntp.org mask 255.255.255.255 nomodify notrap noquery

Con esta configuración el servidor de ntp se sincronizaría a los con los tres servidores que vemos. Así siempre permanecerá perfectamente sincronizado, para que a su vez, todos los equipos de la red puedan sincronizarse y tener todos los mismos controles horarios.

ZONA INTRA FIREWALL

Proxy

Solución de mercado elegida

SW libre en Linux (Squid y Dansguardian)

Características

Tal y como citan en *[22]*, squid es el servidor proxy cache por excelencia en el mundo del software libre, tiene un desarrollo activo de más de 10 años, con un gran soporte tanto por los desarrolladores como por la comunidad, algunas de las características principales de Squid son:

- Liberado bajo la Licencia *GNU General Public License* (GPL).
- Viene incluido y soportado en la mayoría de distribuciones GNU/Linux.
- Soporta los protocolos IPv4 e IPv6.
- Proxy para los protocolos HTTP, HTTPS, FTP y GOPHER.
- Soporte otros Protocolos como ICP, ICAP y WCCP.
- Cache de consultas DNS.

- Cache de contenido para aceleración web con soporte de diferentes sistemas de archivos para el almacenamiento del cache.
- Controles de acceso avanzados basados en ACLs.
- Soporta diferentes esquemas de autenticación.
- Soporta diferentes métodos de autorización.
- Registro de logs y soporte SNMP.
- Soporte de plugins para autenticación de usuarios y grupos.
- Integración de filtros de URLs y contenido como squidGuard y DansGuardian.

Como elemento de filtrado de contenidos se propone la utilización de DansGuardian, un proxy de filtrado, que es capaz de ejecutarse en una gran variedad de sistemas operativos (Linux, FreeBSD, OpenBSD, NetBSD, Mac OS X, HP UX y Solaris). DansGuardian se integra perfectamente con Squid, y puede realizar el filtrado de acuerdo con los siguientes métodos:

- Filtrado de URL (Uniform Resource Locator) dominio; DansGuardian es capaz de gestionar listas muy largas de sitios "prohibidos".
- Filtrado por contenido, lo cual permitirá bloquear páginas obscenas o cuyo contenido puede resultar ofensivo.
- Filtrado tipo PICS (Platform for Internet Content Selection); muchos sitios Web clasifican las páginas que publican de acuerdo con un

sistema que introduce palabras como "desnudez (nudity)", "violencia (violence)" o "sexo (sex)" en las propias páginas, y que pueden ser utilizadas por los clientes para controlar el acceso a determinado tipo de páginas en función de estos criterios. DansGuardian "entiende" este sistema de clasificación y puede actuar de acuerdo con él.

- Filtrado MIME (Multipurpose Internet Mail Extensions), controlando el acceso por medio de la clasificación de acuerdo con este formato.

- Filtrado por extensión de fichero.

- Limitador de operaciones POST, permitiendo bloquear o limitar la subida (upload) de información a la Web.

  Además, DansGuardian dispone de un mecanismo de excepciones que permite que ciertos dominios, direcciones IP o usuarios puedan "saltarse" los mecanismos de bloqueo.

  El mecanismo de registro (logging) que ofrece DansGuardian permite configurarlo de modo que sólo se generen registros de los contenidos textuales, reduciendo así la cantidad de información que se guarda por página (evitando, por ejemplo, guardar información de registro sobre las imágenes de una página).

DansGuardian es altamente configurable, ofreciendo al administrador un enorme control sobre lo que quiere o no bloquear.

Las **principales características de DansGuardian** son las siguientes:

- Su coste es mucho menor que el de otras herramientas de filtrado de contenidos comerciales.

- Puede controlar la publicidad mediante el uso de listas negras.
- Puede filtrar páginas de texto y HTML de acuerdo con su potencial contenido obsceno (sexual, racial, violento, etc).
- Usa un sofisticado sistema de pesos para reducir falsos positivos y falsos negativos a la hora de bloquear una página.
- Puede utilizar el sistema PICS como mecanismo de control de bloqueo.
- Puede filtrar de acuerdo con la extensión MIME o extensión de un fichero.
- Es capaz de filtrar URLs de acuerdo con expresiones regulares.
- El filtrado de URL es compatible con las "listas negras" que utiliza squidGuard.
- El mecanismo de filtrado URL es capaz de bloquear páginas a través de conexiones cifradas (https).
- Puede trabajar también en el denominado modo de "lista blanca" (White list), de acuerdo con el cual todo es bloqueado salvo aquello que está en la lista.
- Puede bloquear URLs referenciadas por IP.
- El mecanismo de registro (logging) produce una salida "fácil de leer".
- Puede generar (de forma opcional), registros en formato CSV, para su posterior uso con sistemas como bases de datos.

- Puede registrar el nombre de usuarios, bien utilizando Ident o bien, utilizando un mecanismo básico de proxy.

- Permite anular el filtrado para ciertos sitios o partes de los mismos, direcciones IP de los navegadores o determinados nombres de usuario.

- Puede bloquear direcciones IP origen o usuarios específicos.

- Puede bloquear la subida de contenido a la Web, como por ejemplo, los adjuntos de Hotmail.

- Puede trabajar en modo "silencioso" (stealth), registrando todo lo que bloquearía si funcionara el bloqueo, pero no bloqueando en realidad nada.

- Esta funcionalidad permitiría monitorizar las acciones de los usuarios sin que estos lo supieran.

- Hace uso de un algoritmo avanzado para identificar texto "mezclado" con blancos y código HTML en las páginas Web.

- Pueden usarse los conjuntos de caracteres Big5, Unicode o top-bit en los textos de búsqueda.

- El filtrado de URL es mucho más rápido que el de squidGuard.

- La eficiencia del código permite que las listas de configuración pueden llegar a tener cientos de miles entradas.

- Es 100% código C++, que compila también con la nueva versión de GCC 3.

- Puede obligarse a releer la configuración de filtrado mediante el envío al proceso de una señal HUP.

- Se integra perfectamente con Squid y Oops.

- No requiere ninguna librería adicional, como ocurría en las primeras versiones, y por tanto, se instala mucho más fácilmente, distribuyéndose también como paquete RPM de Red Hat.

- Esta versión incorpora soporte para la línea de cabecera HTML Forwarded- For de Squid.

- Soporta código HTML comprimido (Conteng-Encoding gzip).

- Puede configurarse de modo que escuche en una sola dirección IP del sistema donde se ejecuta.

En la siguiente figura se muestran una pantalla con información de bloqueo generada por DansGuardian. Cabe decir que esta pantalla será modificable para cada entorno en el que se implante.

Como elemento para la administración de Squid, se propone Webmin, una interfaz Web genérica para la administración de sistemas Unix (cuentas de usuario, servidor Apache, DNS...) y que también dispone de un módulo para la gestión y administración de Squid.

El módulo Webmin Squid proporciona acceso a todas las opciones de configuración del Proxy Squid. Es posible, con este módulo, configurar las ACLs del servicio de proxy, añadir espacio al pool de caché, configurar opciones de aceleración o cambiar las políticas de refresco de la caché. También, proporcionan un acceso a la herramienta de gestión de estadísticas cachemgr.cgi, y, por supuesto, la posibilidad de parar y arrancar el propio servidor.

A continuación se muestra el aspecto de la página principal de Webmin-Squid:

Ambos servidores proxy se instalarán también sobre servidores HP ML 330 G6, ya que el servicio requiere la potencia de dicho servidor.

A continuación se muestran las características más importantes del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Xeon® E5606 (4 núcleos, 2,13 GHz, 12 MB L3, 80 W)
Número de procesadores	1
Núcleo de procesador disponible	4
Memoria, estándar	4 GB
Ranuras de memoria	12 ranuras DIMM
Tipo de memoria	PC3-10600E (UDIMM)
Ranuras de expansión	(4) ranuras PCI-E y (2) ranuras PCI-X opcionales, con ampliador PCI X (usa 1 ranura PCI-E)
Controlador de red	(1) 2 Puertos 1 GbE NC326i
Descripción de unidad	(8) SAS/SATA LFF; sin conexión en caliente o conexión en caliente
Tipo de fuente de alimentación	(1) 460 W sin conexión en caliente, no redundante
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	DVD-ROM SATA media altura
Formato (totalmente configurado)	Bastidor de 5U, torre
Garantía - año(s) (partes/mano de obra/in situ)	3/1/1

Alternativas

La alternativa es BlueCoat CacheFlow

El modelo exacto es el BlueCoat CacheFlow 5000 series

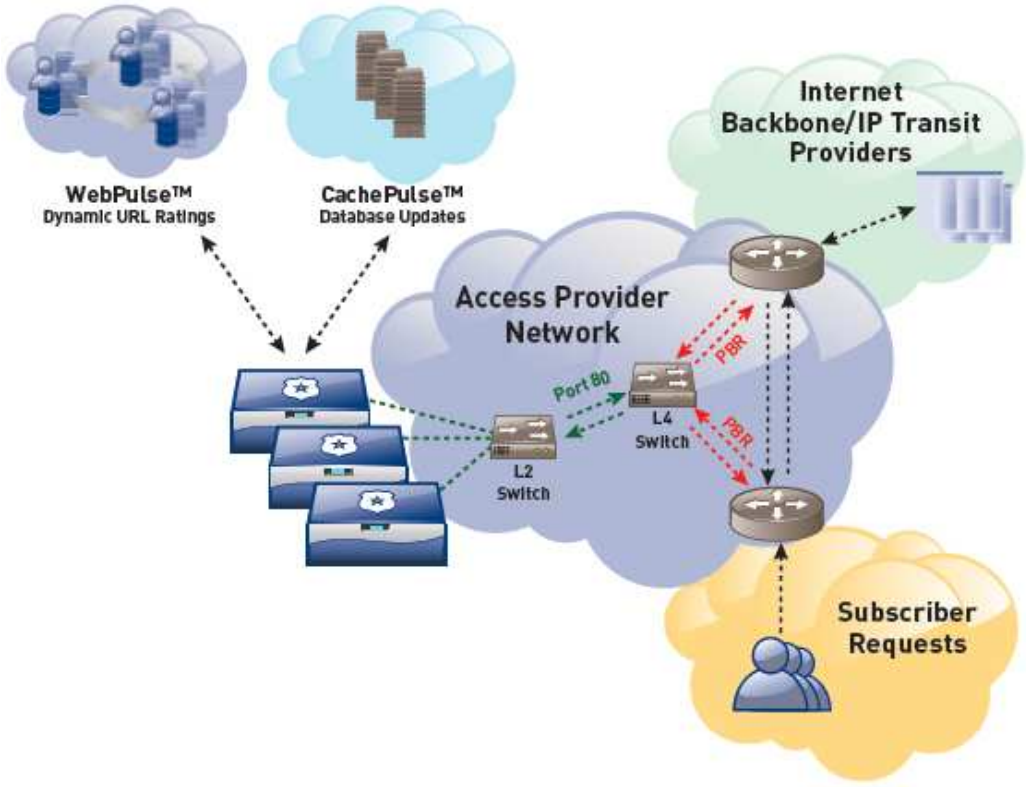
El dispositivo posee las siguientes características hardware, tal y como se puede ver en *[13]*:

Hardware Features	
CPU	Dual 2.6GHz Istanbul (AMD part# 2435) CPUs
Disk Drives	8x1TB SAS
RAM	32GB RAM
Network Interfaces	(4) integrated (on board) 10/100/1000 Base-T NICs, SSL Card, (3) Open PCIE Slots
Optional Cards	None
Optional NICs	Dual port 10G copper card

El BlueCoat CacheFlow permite gestionar un aumento en el tráfico de red. Utilizando una tecnología muy eficaz de almacenamiento en caché Web, CacheFlow ahorra ancho de banda de costosos enlaces internacionales y tráfico de retorno, al tiempo que mejora la experiencia del usuario final Web. A través de una arquitectura escalable de memoria caché de las granjas, se puede

acelerar la entrega de contenido Web 2.0, archivos de gran tamaño y de vídeo. Esto reduce significativamente los costes de infraestructura por el consumo de ancho de banda de control al tiempo que mejora la satisfacción del cliente.

La arquitectura (para un Proveedor de Servicios de Internet) sería la siguiente:



A continuación se van a exponer las características fundamentales de este producto, que se pueden encontrar en *[13]*:

- ***Ahorro de ancho de banda***: Por el almacenamiento de contenido en caché dentro de la región y más cerca del usuario, el dispositivo CacheFlow reduce drásticamente el consumo de ancho de banda. Esto se traduce en un rápido retorno sobre la inversión y un importante ahorro de costes a largo plazo para los proveedores de servicios de ancho de banda internacional, así como la reducción del tráfico backhaul en los enlaces internos.

- ***Aceleración Web 2.0 y multimedia***: CacheFlow permite cachear los sitios Web 2.0, y sitios multimedia más visitados incluyendo los sitios de intercambio de archivos y video. El almacenamiento en caché permite ahorrar ancho de banda mientras aumenta la experiencia del usuario.

- ***Asegura la eficacia caché***: BlueCoat aprovecha CacheFlow CachePulse ™ para las actualizaciones automáticas, basadas en la red como los cambios de Web para asegurarse de que el dispositivo cachee de forma efectiva el contenido de forma coherente y que así permita ahorrar un mayor ancho de banda.

- ***Filtra y securiza el tráfico Web***: Al activar la función de BlueCoat WebFilter™, CacheFlow filtra y protege el tráfico web, incluyendo contenidos no deseados y los sitios infectados con malware. CacheFlow también le permite crear excepciones personalizadas y listas de bloqueo de sitios específicos, así como aprovechar la lista de Internet Watch Foundation para filtrar contenido ilegal.

- ***Escalable con crecimiento de usuarios y tráfico***: CacheFlow fue diseñado para entornos de alto rendimiento de proveedores de servicios con la capacidad de escalar a tráficos multi-gigabit a través del uso de las granjas caché. CacheFlow ofrece dos interfaces de 1GigE y 10GigE para los requisitos de infraestructura de alta velocidad de la red y una estrecha integración con los swichtes para una mayor escalabilidad y rendimiento.

- ***Administración y reporte de tráfico Web***: CacheFlow proporciona una administración a través de una consola Web muy intuitiva, y unas herramientas de comandos de línea para administrar el aparato. Para el monitoreo continuo, CacheFlow se integra a través de SNMP a otras

soluciones de gestión de red y soporta el logeo de eventos a través de syslog.

- ***Soporte***: Para este dispositivo, BlueCoat ofrece un soporte 24/7 que está soportado por un equipo dedicado de expertos. Además el aparato incluye funciones integradas para solucionar y mitigar proactivamente los problemas y acelerar la resolución de éstos.

Solución de mercado elegida

Esafe Web Security Gateway

Características

Esafe Web Security Gateway es un antivirus que trabaja en tiempo real filtrando el tráfico que va entrando en la red, ya sea tráfico HTTP o FTP, en busca de trazas de cualquier rastro de malware, tráfico inapropiado, o contenidos y aplicaciones que no estén permitidos en la organización donde se encuentre instalado. Además supervisa todo el tráfico saliente con un avanzado sistema de prevención de fuga de datos (DLP), para no permitir que determinados datos puedan salir fuera de la organización.

Esafe Web Security Gateway está formado por siete módulos, los cuales se detallan en *[15]*:

Security (includes anti-malware, anti-spyware, and anti-virus):

A diferencia de otras soluciones que se centran principalmente en la inspección de los archivos descargables en busca de virus, eSafe ofrece (con el motor de Kaspersky) la detección malweb (malware web específica).Malweb está oculto dentro del contenido web estándar y está diseñado para explotar varias vulnerabilidades en las aplicaciones habilitadas para Internet, tales como los navegadores, plugins, y cualquier otra aplicación que interactúa con la web.

eSafe es capaz de detectar de forma proactiva los intentos de aprovechar las vulnerabilidades antes de que hayan entrado en la organización, en lugar de detectar el malware cuando se está descargando, lo que podría resultar fatal.

Los dos motores de eSafe proporcionan seguridad doble. El motor de seguridad proactiva utiliza múltiples capas de análisis de inspección profunda de código para bloquear de manera efectiva amenazas de día cero (las que acaban de salir), mientras que el motor de "basados en firmas" (Kaspersky) se basa en las actualizaciones oportunas para bloquear con eficacia los virus conocidos.

eSafe soporta todos los archivos de MS Office y los tipos de archivo de archivos. También evita que el spyware pueda enviar información confidencial, y se actualiza automáticamente cada hora para mantener la seguridad más actualizada disponible.

Algunas características son las siguientes:

- Doble motor antivirus (Esafe y Kaspersky AV)
- Soporta todo tipo de archivos de MS Office
- Se actualiza automáticamente cada hora
- Tecnología de análisis de contenido activo web
- Soporta filtrado de scripts inteligentes
- Realiza detección de ofuscación
- Detecta y bloquea ficheros conocidos de spyware y sitios web.
- Bloquea canales de comunicación y protocolos utilizados por los spyware.
- Evita que los spyware saquen fuera datos confidenciales de la organización.

eSafe Application And Web 2.0 Control

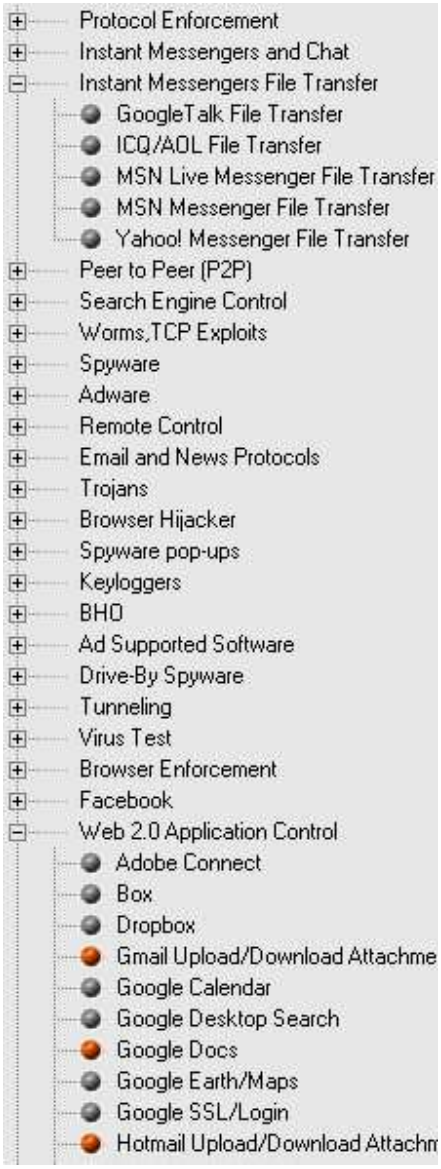
El eSafe Application and Web 2.0 Control proporciona un control granular de aplicaciones web, para poder regular el uso de Internet, y evitar operaciones no autorizadas, no deseado o peligroso que puede conducir a la infección o la fuga de información.

El módulo de control eSafe Web 2.0 impide que la Web 2.0 basada en aplicaciones pueda traspasar las medidas de seguridad existentes y cree agujeros por los que el spyware, troyanos, virus y otros programas maliciosos pueden atacar a la red.

El filtro de aplicación proporciona una completa protección en tiempo real contra aplicaciones maliciosas, peligrosas y no deseadas, con más de 500 protocolos de aplicación en más de 20 categorías. Mediante el seguimiento, control y bloqueo de aplicaciones en el Gateway, la red será inspeccionada en tiempo real, permitiendo sólo el uso de aplicaciones permitidas, sin dejar de ser completamente transparente para los usuarios.

A continuación se enumerarán algunas características:

- Política basada en el control de:
- Malware / spyware "call-home" de comunicación.
- El intercambio de archivos P2P
- Mensajería instantánea de chat y transferencia de archivos
- Protocolo de túnel sin autorización
- Aplicación (capa 7) del protocolo de aplicación
- Compatible con todos los sitios más populares Web 2.0
- Evita el phising Web 2.0, malware, exploits, etc
- Evita traspasar la seguridad y filtrado de contenido las políticas de proxys anónimos y aplicaciones
- Seguridad granular y políticas de spam a los usuarios de LDAP / AD y grupos
- Políticas granulares para el adecuado uso de Web 2.0 en una organización:


Protocol Enforcement
Instant Messengers and Chat
Instant Messengers File Transfer
GoogleTalk File Transfer
ICQ/AOL File Transfer
MSN Live Messenger File Transfer
MSN Messenger File Transfer
Yahoo! Messenger File Transfer
Peer to Peer (P2P)
Search Engine Control
Worms,TCP Exploits
Spyware
Adware
Remote Control
Email and News Protocols
Trojans
Browser Hijacker
Spyware pop-ups
Keyloggers
BHO
Ad Supported Software
Drive-By Spyware
Tunneling
Virus Test
Browser Enforcement
Facebook
Web 2.0 Application Control
Adobe Connect
Box
Dropbox
Gmail Upload/Download Attachme
Google Calendar
Google Desktop Search
Google Docs
Google Earth/Maps
Google SSL/Login
Hotmail Upload/Download Attachm

Esta solución se implantará sobre un servidor HP DL 120 G7, ya que por especificaciones técnicas cumple con los requisitos necesarios para el servicio.

A continuación se muestran las principales características del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Core™ i3 2100 (2 núcleos, 3,1 GHz, 3 MB, 65 W, 1333/t)
Número de procesadores	1
Núcleo de procesador disponible	2
Memoria, estándar	2 GB
Ranuras de memoria	4 ranuras DIMM
Tipo de memoria	PC3-10600E DDR3 UDIMMs
Ranuras de expansión	2
Controlador de red	(2) 1 puerto NC112i 1 GbE
Tipo de fuente de alimentación	(1) detección automática de 400 W, cumple con la marca CE
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	Ningún estándar de suministro
Formato (totalmente configurado)	1U
Garantía - año(s) (partes/mano de obra/in situ)	1/1/1

La alternativa es Optenet WebSecure

A continuación se muestran las funcionalidades de esta solución, que se pueden encontrar en *[17]*:

SEGURIDAD

- *Seguridad Web*: Preparada para la Web 2.0. La solución de filtrado web y antimalware de Optenet, basada en el analizador semántico multilingüe MIDAS™ (Multi-content Inspection & Dynamic Analysis System) y el sistema de análisis de amenazas GIANT™ (Global Intelligence Acquisition Network for Threats), clasifica y bloquea con total precisión el acceso a sitios web no adecuados.

- *Protección contra Malware:* La Seguridad Web se complementa con el motor antivirus más avanzado de Kaspersky Labs y Sophos, para ofrecer una protección superior frente a virus, spyware, troyanos, gusanos y más.

- *Antiphishing:* WebSecure incorpora un motor de antiphishing que analiza tráfico web y email para identificar actividades sospechosas y proteger de ataques de phishing.

- *Cortafuegos:* Completo. Ofrece la posibilidad de filtrar grupos de servicios de nivel 7 de Internet (Gestión de Aplicaciones).

- *Protección del menor:* Con más de una década de experiencia en protección del menor, Optenet ha recibido las más altas valoraciones en estudios especializados como el "Safer Internet Plus Programme", auditado cada año por Deloitte para la Comisión Europea. Además, Optenet trabaja con ONGs y Organizaciones para combatir el flujo constante de amenazas en línea y crear un entorno seguro para los menores. El departamento de I+D está siempre innovando y desarrollando nuevas tecnologías que salvaguardan a los internautas contra cibercriminales y protegen a los menores de contenidos nocivos tales como contenidos para adultos y cyber-bulling.

RED

- *Aceleración de tráfico:* Reduce el ancho de banda y la latencia para evitar la congestión del tráfico.

- *Administración de QoS y Gestión de Ancho de Banda:* Estas dos funcionalidades, disponibles para administradores, permiten la definición de políticas granulares para controlar los niveles de *servicio y limitar la tasa de bits del tráfico de la red al cliente y la dirección IP.*

SERVICIOS

- *Servicio de desbloqueo online*: Confiere al sistema una mínima tasa de falsos positivos, resolviendo cualquier error de sobre bloqueo en menos de 15 minutos.

- *Servicio de notificaciones:* Ofrece a los administradores un poderoso mecanismo para enviar notificaciones automáticas y personalizadas a sus usuarios basadas en la combinación de múltiples políticas y análisis de tráfico.

- *Informes y monitorización en tiempo real:* Todas las soluciones empresariales de Optenet incluyen el sistema de informes y monitorización en tiempo real más rápido disponible. Los informes, respaldados por una base de datos que incorpora la solución sin necesidad de licencias adicionales, se pueden personalizar en función de las necesidades empresariales.

ADMINISTRACIÓN CENTRALIZADA POR CAPAS

Administración central y operaciones distribuidas

Mediante una potente y a la vez sencilla consola de gestión centralizada, la administración de políticas para varias ubicaciones y varias máquinas no implica ningún esfuerzo. Los administradores pueden usar la consola para definir y ejecutar políticas de bloqueo sin límite, aplicables en una escala global, independientemente de la infraestructura de la red.

Administración por capas eficiente y efectiva

Los administradores pueden configurar de forma sencilla y efectiva y personalizar las políticas de acceso por usuario, grupo, estación de trabajo o

red, ya sea de forma local o global. De esta forma, resulta sencillo permitir un nivel de acceso para todas las ubicaciones o proporcionar administración local con diferentes niveles de acceso, de acuerdo con necesidades específicas. El sistema de administración por capas proporciona una flexibilidad que permite a las empresas protegerse con la máxima granularidad y eficiencia.

TECNOLOGÍA DE CLASIFICACIÓN DINÁMICA DE CONTENIDO

En la era de la Web 2.0, los usuarios finales contribuyen activamente a dinamizar Internet. Como resultado, las empresas necesitan soluciones de seguridad con los niveles más altos de protección dinámica para proteger sus redes. Este dinamismo exige, por otro lado, tener la capacidad de clasificar el tráfico en tiempo real. Optenet WebSecure™ es una solución inteligente, rentable y muy precisa de seguridad web que protege frente a malware y frente a contenido ilegal e inapropiado. Sólo Optenet WebSecure™ puede proporcionar a los administradores de sistemas la tecnología necesaria para configurar y controlar políticas que garanticen una protección en tiempo real a sus clientes finales, frente a contenido malicioso e inapropiado y sin impactar en su experiencia en la navegación.

Optenet GIANT™ recibe información constante de fuentes de Internet de todo el mundo y envía esas actualizaciones a cada instancia de la solución de Optenet, garantizando el correcto bloqueo de las nuevas amenazas al poco de aparecer. Por su parte, **Optenet MIDAS™** identifica con total precisión el contenido inadecuado, ilegal y dañino.

Un Motor integrado de inspección profunda de paquetes, **CCOTTA™**, analiza el tráfico en tiempo real y lo redirige a los servicios de filtrado adecuados, sin requerir ningún hardware DPI externo.

RED DE SERVIDORES

Servidores RADIUS

Solución de mercado elegida

SW libre en Linux (free radius y dialupadmin)

Características

Para la solución Radius se ha optado por instalar en un servidor HP un sistema operativo Debian, en el que se instalarán los siguientes paquetes reseñables:

- ***HeartBeat***: como sistema de alta disponibilidad, para ello heartbeat monitoriza de manera permanente la comunicación entre los nodos por el interface de servicio, junto con una comunicación alternativa por puerto serie.

- ***Freeradius***: Como sistema de de autenticación, autorización y accounting basado en el protocolo Radius, además se han incluido el paquete freeradius-mysql para utilizar la base de datos MySQL como backend de almacenamiento del servidor radius

- ***Freeradius-dialupadmin***: Como interface Web de administración del servidor radius.

- ***Mysql-server***: como backend de almacenamiento para el servicio radius.

- ***Apache-ssl***: como servidor web seguro servicio de administración web freeradius-dialupadmin.

La solución de sistema radius implantada se basa el producto freeradius utilizando como backend de almacenamiento de los usuarios, parámetros asociados a estos y el accounting registrado por su actividad en una base de datos MySQL, esta solución además permite la integración de la solución con el interface web dialupadmin y la posibilidad de replicar la información de manera automatizada entre el servidor primario y el de backup.

HeartBeat

La integración de la solución en Alta disponibilidad, para el servicio radius implantada, consiste en la utilización de HeartBeat para mover entre los dos equipos la IP de servicio, de forma que en condiciones nominales la IP es levantada por el primario, y en caso de malfuncionamiento de este nodo la IP de servicio será publicadas por el nodo secundario.

Freeradius.

La configuración del servidor freeradius parte del archivo /etc/freeradius/radiusd.conf, no obstante desde este fichero se pueden incluir otros, para una mejor organización de la configuración y compatibilidad con versiones anteriores.

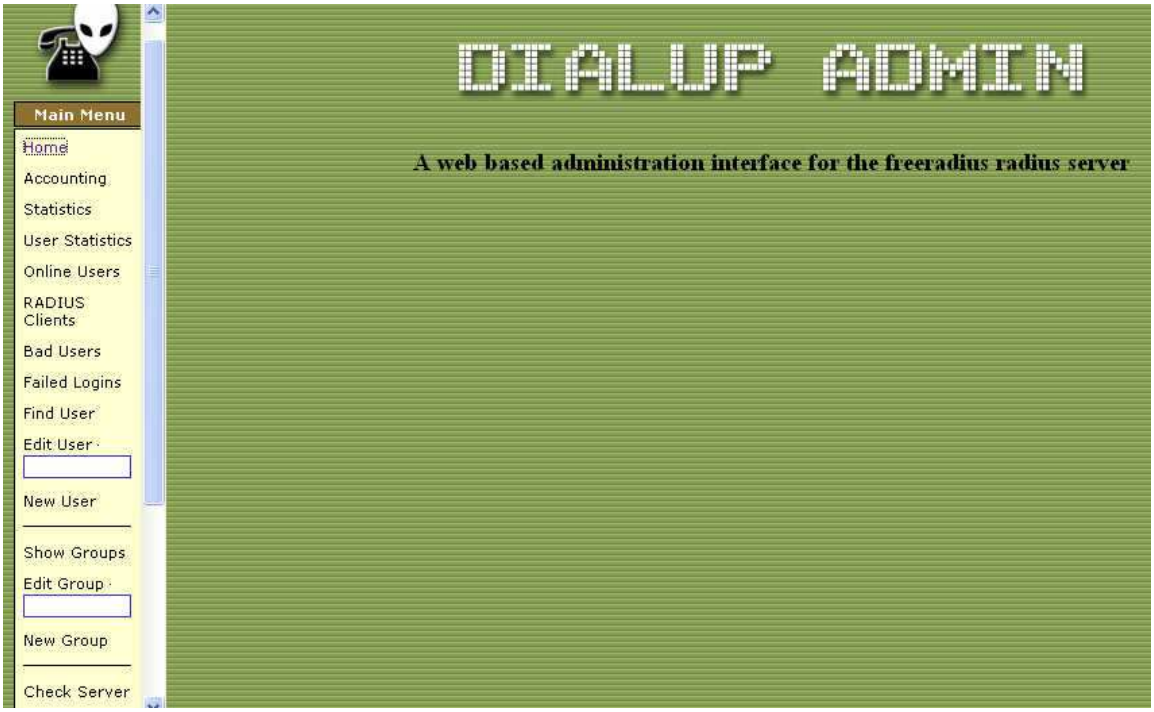
Freeradius-dialupadmin

Dialupadmin es un interface web para administrar gráficamente la provisión de usuarios del servidor radius, así como la monitorización y consulta de registros de acceso. Esta configuración se basa en el archivo admin.conf que a su vez incluye los siguientes archivos:

/etc/freeradius-dialupadmin/sql.attrmap
/etc/freeradius-dialupadmin/accounting.attrs
/etc/freeradius-dialupadmin/extra.ldap-attrmap
/etc/freeradius-dialupadmin/user_edit.attrs
/etc/freeradius-dialupadmin/sql.attrmap
/etc/freeradius-dialupadmin/default.vals
/etc/freeradius-dialupadmin/auth.request

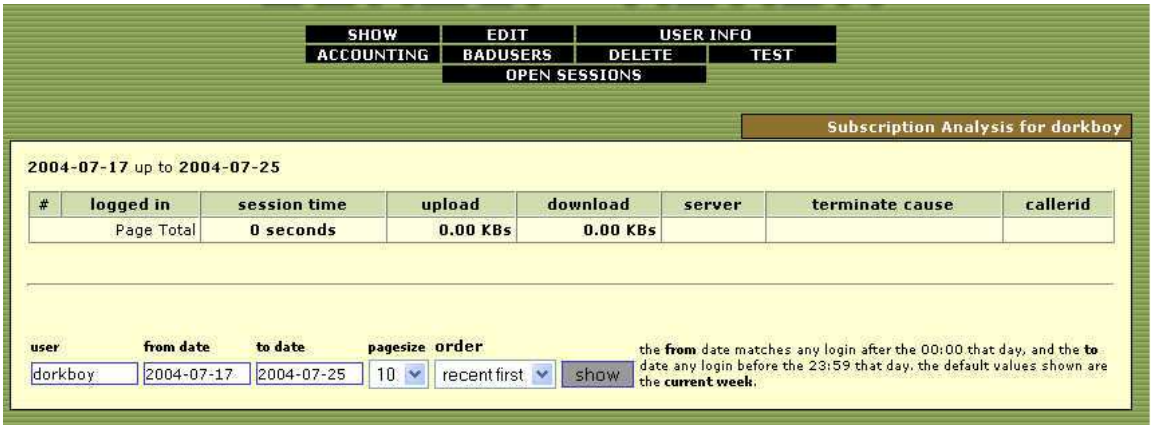
A continuación se muestran unas capturas de pantalla del interfaz web:

Pantalla principal



Modificación de usuario

Información de usuario



Generador de reportes

Mysql-server

La instalación de mysql se realiza de manera estándar, modificándose únicamente el archivo /etc/mysql/my.cnf para comentar la línea

#bind-address = 127.0.0.1

De forma que se pueda acceder vía red a la base de datos, tal y como se requiere para la replicación, además se han incluido las siguientes líneas para permitir la replicación entre servidores.

Además se debe crear la base de datos radius (CREATE DATABASE RADIUS;) y asignar los permisos a la replicación (GRANT REPLICATION SLAVE ON *.* TO usuario@IP_NODO IDENTIFIED BY 'passwd';)

Las bases de datos de los dos servidores se configurarán como "Dual-Master", en la que los dos son maestros y se replican mutuamente.

Apache-ssl

La instalación de apache-ssl que se ha de desplegar, corresponderá a la estándar de la distribución Linux en la que se instale el servidor. Únicamente se incluirá el archivo /etc/apache-ssl/conf.d/dialupadmin.conf para añadir la configuración de freeradius-dialupadmin junto con la creación de los usuarios mediante al herramienta htpasswd.

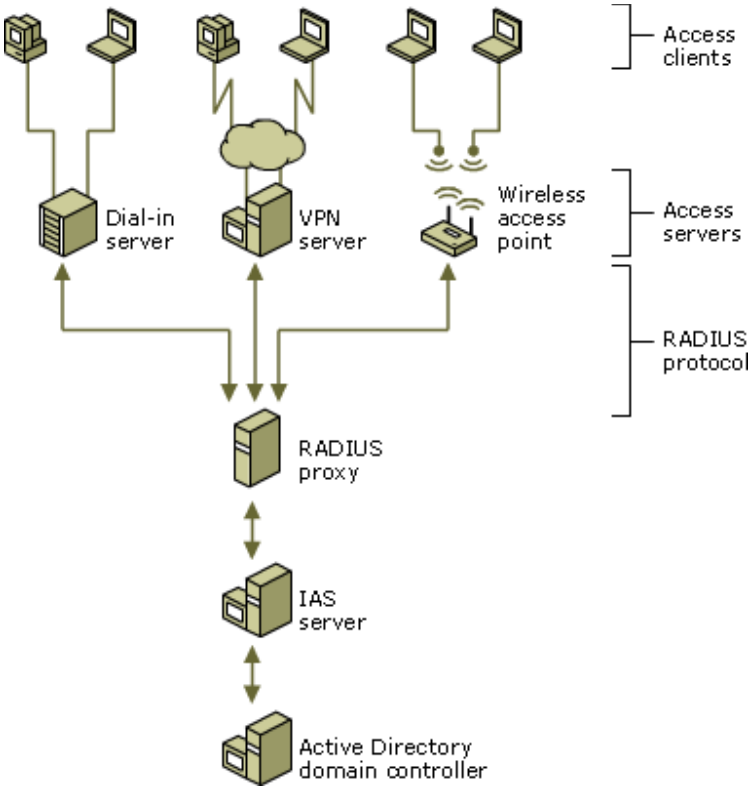
Alternativas

Microsoft IAS como servidor RADIUS *[23]*

El Servicio de autenticación de Internet (IAS, Internet Authentication Service) se puede utilizar como servidor RADIUS para la autenticación, autorización y administración de cuentas de clientes RADIUS. Los clientes RADIUS pueden ser servidores de acceso o proxy RADIUS. Cuando el Servicio de autenticación de Internet (IAS) se utiliza como servidor RADIUS, proporciona lo siguiente:

- Un servicio central de autenticación y autorización para todas las peticiones de acceso enviadas por clientes RADIUS.
  Para autenticar las credenciales de usuario de un intento de conexión, IAS utiliza un dominio de Microsoft® Windows NT® Server 4.0, un dominio de Active Directory® o el Administrador de cuentas de seguridad (SAM, Security Accounts Manager) local. Para autorizar la conexión, IAS utiliza las propiedades de marcado de la cuenta de usuario y las directivas de acceso remoto.
- Un servicio central de registros de administración de cuentas para todas las solicitudes de administración de cuentas enviadas por clientes RADIUS.
  Las solicitudes de administración de cuentas se almacenan en un registro local para su posterior análisis.

En la siguiente ilustración se muestra IAS como servidor RADIUS para una variedad de clientes de acceso y un proxy RADIUS. IAS utiliza un dominio de Active Directory para la autenticación de las credenciales de usuario de los mensajes de petición de acceso RADIUS entrantes.



Cuando se utiliza IAS como servidor RADIUS, los mensajes RADIUS proporcionan autenticación, autorización y administración de cuentas de las conexiones de acceso a la red de la manera siguiente:

1. Los servidores de acceso, como los servidores de acceso telefónico a redes, servidores VPN y puntos de acceso inalámbricos, reciben peticiones de conexión de los clientes de acceso.
2. El servidor de acceso, configurado para utilizar RADIUS como protocolo de autenticación, autorización y administración de cuentas, crea un mensaje de petición de acceso y lo envía al servidor IAS.
3. El servidor IAS evalúa el mensaje de petición de acceso.

4. Si es necesario, el servidor IAS envía un mensaje de desafío de acceso al servidor de acceso. El servidor de acceso procesa el desafío y envía una petición de acceso actualizada al servidor IAS.
5. Se comprueban las credenciales de usuario y se obtienen las propiedades de acceso telefónico de la cuenta de usuario mediante una conexión segura a un controlador de dominio.
6. El intento de conexión se autoriza con las propiedades de acceso telefónico de la cuenta de usuario y las directivas de acceso remoto.
7. Si se autentica y autoriza el intento de conexión, el servidor IAS envía un mensaje de aceptación de acceso al servidor de acceso. Si no se autentica ni se autoriza el intento de conexión, el servidor IAS envía un mensaje de rechazo de acceso al servidor de acceso.
8. El servidor de acceso completa el proceso de conexión con el cliente de acceso y envía un mensaje de solicitud de administración de cuentas al servidor IAS, en el cual se registra el mensaje.
9. El servidor IAS envía una respuesta de administración de cuentas al servidor de acceso.

Nota

- El servidor de acceso también envía mensajes de solicitud de administración de cuentas en los siguientes casos:
  - Durante el tiempo en que se establece la conexión.
  - Cuando se cierra la conexión del cliente de acceso.
  - Cuando se inicia y se detiene el servidor de acceso.

Puede utilizar IAS como servidor RADIUS en los siguientes casos:

- Utiliza un dominio de Microsoft® Windows NT® Server 4.0, un dominio de Active Directory o el Administrador de cuentas de seguridad (SAM) local como base de datos de cuentas de usuario de los clientes de acceso.

- Utiliza el servicio Enrutamiento y acceso remoto de Microsoft® Windows Server® 2003, Standard Edition, Windows Server 2003, Enterprise Edition, Windows Server 2003, Datacenter Edition o Windows 2000 en varios servidores de acceso telefónico, servidores VPN o enrutadores de marcado a petición y desea centralizar la configuración de las directivas de acceso remoto y el registro de conexiones para la administración de cuentas.

- Subcontrata el acceso telefónico, VPN o inalámbrico a un proveedor de servicios. Los servidores de acceso utilizan RADIUS para autenticar y autorizar las conexiones que realizan los miembros de la organización.

- Desea centralizar la autenticación, la autorización y la administración de cuentas en un grupo heterogéneo de servidores de acceso.

Nota

Puede configurar IAS en Windows Server 2003, Standard Edition, con un máximo de 50 clientes de RADIUS y 2 grupos de servidores RADIUS remotos.

Puede definir un cliente de RADIUS mediante un nombre de dominio completo o una dirección IP, pero no puede definir grupos de clientes de RADIUS mediante un intervalo de direcciones IP. Si el nombre de dominio completo de un cliente de RADIUS se resuelve como varias direcciones IP, el servidor IAS utiliza la primera dirección IP devuelta en la consulta DNS. Con IAS en Windows Server 2003, Enterprise Edition, y Windows Server 2003, Datacenter Edition, puede configurar un número ilimitado de clientes de RADIUS y grupos de servidores RADIUS remotos. Además, puede configurar clientes de RADIUS si especifica un intervalo de direcciones_IP.

Los servidores radius se instalarán sobre dos servidores HP DL 120 G7, ya que son servidores lo suficientemente potentes para ello.

A continuación se muestran las principales características del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Core™ i3 2100 (2 núcleos, 3,1 GHz, 3 MB, 65 W, 1333/t)
Número de procesadores	1
Núcleo de procesador disponible	2
Memoria, estándar	2 GB
Ranuras de memoria	4 ranuras DIMM
Tipo de memoria	PC3-10600E DDR3 UDIMMs
Ranuras de expansión	2
Controlador de red	(2) 1 puerto NC112i 1 GbE
Tipo de fuente de alimentación	(1) detección automática de 400 W, cumple con la marca CE
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	Ningún estándar de suministro
Formato (totalmente configurado)	1U
Garantía - año(s) (partes/mano de obra/in situ)	1/1/1

RED DE GESTIÓN

Firewall de Gestión

Solución de mercado elegida

CheckPoint FW1, de CheckPoint

Características

Check Point tiene todas sus soluciones de seguridad separadas en "Software Blades".

Un Software Blade es un elemento de seguridad lógico que es independiente, modular y gestionado de forma centralizada. Puede ser activado y configurado rápidamente en una solución basada en las necesidades empresariales específicas. Y a medida que evolucionan las necesidades, los blades pueden activarse rápidamente para extender la seguridad a una configuración existente del mismo hardware.

Dichos blades se pueden combinar para crear una solución de seguridad personalizada. Se pueden adquirir de forma independiente o como paquetes predefinidos.

A continuación se detallan las características de los Software Blades, que se pueden encontrar en *[24]*:

- **Flexibilidad** - Proporciona el nivel óptimo de protección en el nivel adecuado de inversión.

- **Capacidad de gestión** - Permite la implementación rápida de servicios de seguridad. Aumenta la productividad mediante la gestión centralizada del blade.
- **Seguridad Total -** Proporciona el nivel óptimo de seguridad, en todos los puntos de aplicación, y en todas las capas de la red.
- **Reducir el TCO -** Protege la inversión mediante la consolidación y el uso de la infraestructura de hardware existente.
- **Rendimiento garantizado -** Permite el aprovisionamiento de recursos que garantizan los niveles de servicio.

Existen los siguientes Software Blades:

- Firewall
- IPSEC VPN
- Mobile Access
- Identity Awareness
- Application Control
- IPS
- DLP
- Web Security
- URL Filtering
- Anti-Bot
- Antivirus & Anti-Malware
- Anti-Spam & Email Security
- Advanced Networking
- Acceleration & Clustering
- Voice over IP (VoIP)
- Security Gateway Virtual Edition

La arquitectura Software Blade de Check Point ofrece de una mejor manera, permitir a las organizaciones adaptar de manera eficiente soluciones específicas que cumplen con las necesidades específicas de negocio de

seguridad. Todas las soluciones son administradas centralmente a través de una única consola que reduce la complejidad de administración. Y a medida que surgen nuevas amenazas, la arquitectura Software Blade de Check Point expande con rapidez y flexibilidad los nuevos servicios, según sea necesario sin necesidad de añadir nuevo hardware ni complicar la administración.

Es la primera arquitectura que ofrece una seguridad total, flexible y manejable para las empresas de cualquier tamaño.

Para ayudar a facilitar la configuración, Check Point ha desarrollado varios paquetes (Security Gateway Systems) predefinidos compuesto por un contenedor de Software Blades:

Oficinas pequeñas y sucursales

Serie 100 - Una solución de seguridad ideal para la pequeña oficina. Un sistema de un núcleo, limitado a 50 usuarios y recomienda un máximo de 8 puertos:

- **SG103:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness.
  Descripción: ofrece un nivel de seguridad de pasarela para proporcionar una protección a oficinas o sucursales pequeñas.

- **SG108:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware
  Descripción: XTM (gestión de amenazas extensible) ideal que proporciona seguridad total de pasarela para pequeñas oficinas y sucursales.

Medianas empresas y oficinas

Serie 200 - Una plataforma de seguridad económica para medianas empresas. Un sistema de dos núcleos, con límite de 500 usuarios o usuarios ilimitados, y se recomienda un máximo de 12 puertos:

- **SG205i:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness.
  Descripción: nivel de seguridad gateway para proporcionar una protección fundamental para empresas medianas.

- **SG205U:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness.
  Descripción: nivel de seguridad gateway para proporcionar una protección fundamental para empresas medianas con más de 500 usuarios.

- **SG207i:**
  Software Blades: Firewall, IPSEC VPN, IPS, Application Control, Identity Awareness, Advanced Networking, Acceleration & Clustering.
  Descripción: alto rendimiento de seguridad de gateway para medianas empresas y oficinas con entornos de red exigentes.

- **SG209:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering.

Descripción: XTM (gestión de amenazas extensible) más completo, que ofrece seguridad de gateway con capacidades de alto rendimiento para empresas de tamaño medio.

Oficinas de alto rendimiento de cualquier tamaño

Serie 400 - Diseñado para entornos que exigen un alto rendimiento. Ideal para las redes de campus y grandes centros de datos. Está optimizado para un sistema de 8 núcleos.

- **SG407i:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness, Advanced Networking, Acceleration & Clustering.
  Descripción: alto rendimiento de seguridad de gateway para empresas de cualquier tamaño.

- **SG409:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness, Anti-Spam & Email Security, URL Filtering, Antivirus & Anti-Malware, Acceleration & Clustering.
  Descripción: XTM (gestión de amenazas extensible) más completo, que ofrece seguridad de gateway para oficinas de cualquier tamaño que requieran un alto rendimiento.

Grandes empresas, universidades y data center

Serie 800 - Diseñado para los entornos de rendimiento más exigentes, la Serie 800 de seguridad gateway es ideal para grandes campus y centros de datos. Está optimizado para un sistema de 8 núcleos.

- **SG807:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness, Advanced Networking, Acceleration & Clustering.
  Descripción: seguridad gateway de alto rendimiento para entornos de máxima exigencia.

Serie 1200 - Diseñado para los mayores entornos que exigen los más altos rendimientos.

- **SG1207:**
  Software Blades: Firewall, VPN, IPS, Application Control, Identity Awareness, Advanced Networking, Acceleration & Clustering.
  Descripción: seguridad de gateway para el mayor rendimiento en los entornos con más altas exigencias.

Los Software Blades pueden desplegarse en appliance propios de Check Point o en servidores de terceros. Los nuevos blades pueden ser añadidos simplemente activándolos en el software, sin necesidad de ningún otro hardware, firmware o driver adicional. Esto hace que las empresas u organizaciones puedan desplegar políticas de seguridad de forma dinámica con el menor coste que ello constituye.

El Check Point Firewall Software Blade incorpora toda la potencia y la capacidad de la solución revolucionaria FireWall-1 (tecnología de inspección de estado), mientras que la adición del conocimiento de identidad del usuario proporciona una granularidad de gestión de eventos y aplicación de políticas.

A continuación se detallan algunas características del Check Point Firewall Software Blade:

- *Control de acceso*: permite a los administradores de red controlar de forma segura el acceso a los clientes, servidores y aplicaciones, con

una visibilidad detallada de los usuarios, grupos, aplicaciones, equipos y tipos de conexión, el firewall de Check Point Software Blade permite a los administradores de red proporcionar una protección superior a través de una seguridad gateway completa.

- *Conocimiento de usuario y máquina*: el conocimiento de usuarios y máquinas permite realizar definiciones de políticas granulares por usuario y grupo.

  Una integración perfecta y sin agentes con Active Directory proporciona una identificación de usuario completa, permitiendo una simple aplicación basada en la definición de políticas por usuario o grupo directamente desde el servidor de seguridad.

  La identificación de los usuarios puede ser realizada mediante tres métodos simples:
    - Consultando Active Directory
    - A través de un portal cautivo
    - Instalación de una sola vez, de un agente en la máquina cliente

- *Autenticación:* Para garantizar la seguridad de la red, se necesita estar en condiciones de confirmar la identidad de todos los usuarios que intentan acceder a ella. La autenticación asigna permisos de acceso a individuos y grupos, en función de su nivel de responsabilidad y rol dentro de la organización.

  Basado en el conocimiento de la industria de identidad más avanzada, Check Point Firewall Software Blade proporciona capacidades robustas de autenticación para confirmar la identidad de todos los usuarios y establecer sus derechos y privilegios.

El componente de autenticación de Check Point Firewall Software Blade ofrece:

* Múltiples y complementarios métodos para obtener la identidad.
* Integración de la funcionalidad del conocimiento del usuario entre la seguridad de gateway y la management.

- *Network Address Translation (NAT):* Si los equipos tienen direcciones enrutables o no enrutables, los administradores pueden ocultar sus direcciones reales, para asegurarse de que las direcciones no pueden ser vistas desde fuera de la organización o de otras partes de la misma organización. La dirección interna de una red contiene la topología de la red y por lo tanto, ocultando esta información aumenta enormemente la seguridad.

- *Modo Bridge*: Un gateway de seguridad en modo bridge funciona como un firewall normal, inspeccionando el tráfico y bloqueando el tráfico no autorizado o peligroso, y es invisible para todo el tráfico de capa 3. Cuando el tráfico autorizado llega al gateway, se pasa de una interfaz a otra a través de un procedimiento conocido como puente. Crea un puente de capa 2 relacionado entre dos o más interfaces, por lo que todo el tráfico que entra en una interfaz siempre sale por el otro. De esta forma, el firewall puede inspeccionar y reenviar el tráfico sin interferir el enrutamiento IP original.

- *Integrado en la arquitectura Software Blade de Check Point*: Firewall Software Blade está plenamente integrada en la arquitectura Software Blade, ahorrando tiempo y reduciendo sus costes al permitir a los clientes expandir rápidamente las protecciones de seguridad para satisfacer las necesidades cambiantes. Además se incluye en el

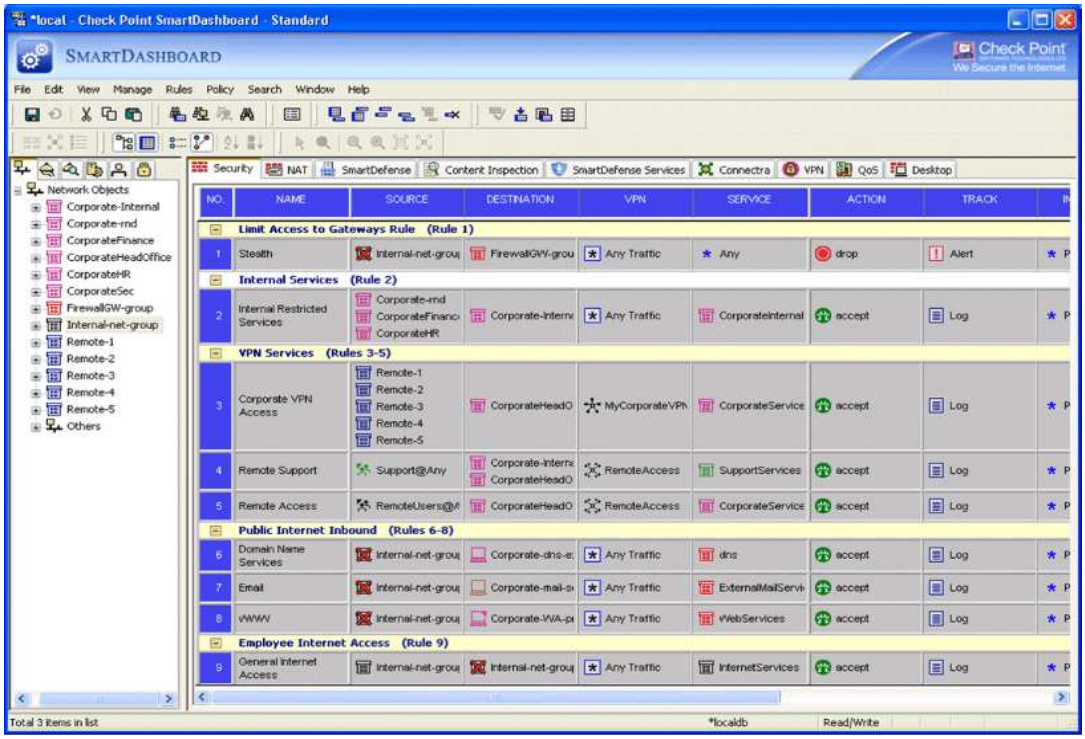
contenedor de Gateway de Seguridad cuando usted compra un producto Gateway Security.

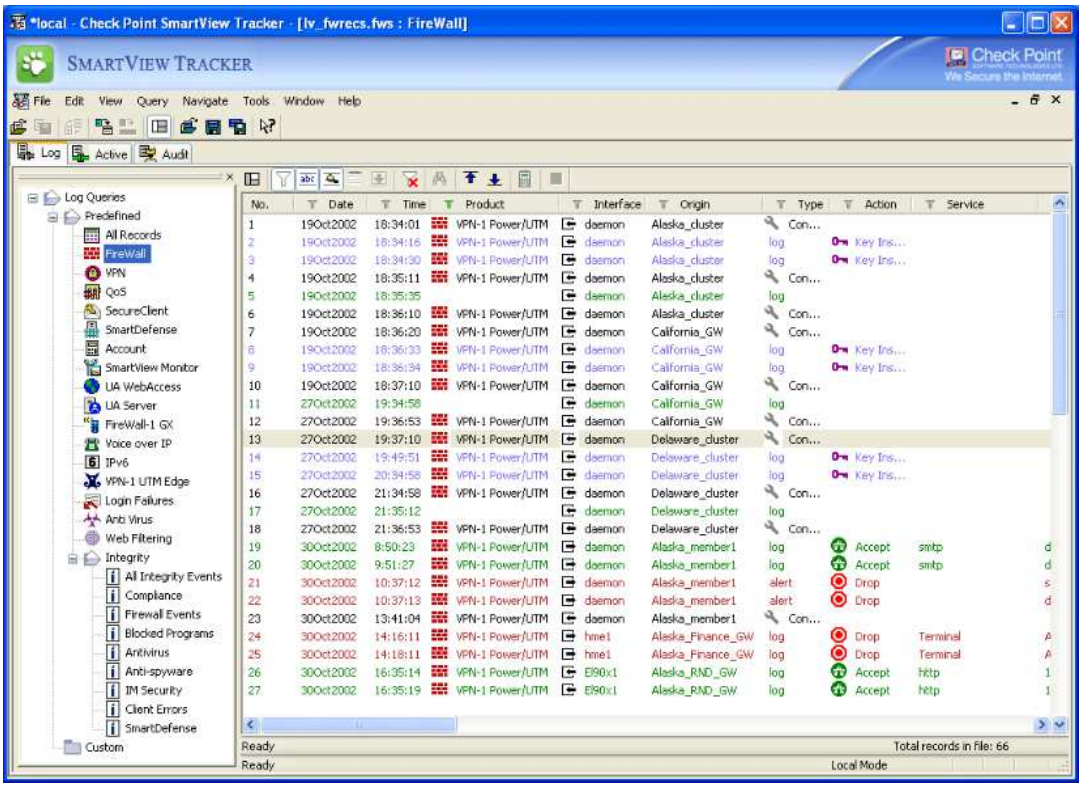
En este cuadro se pueden ver de forma más detallada algunas de sus especificaciones más importantes:

Feature	Details
Protocol/Application Support	500 plus protocol types
VoIP Protection	SIP, H.323, MGCP and SIP with NAT support
Network Address Translation	Static/hide NAT support with manual or automatic rules
DHCP Gateways	Security gateways can have dynamic IP addresses
VLAN	Up to 256 VLANs per interface
Link Aggregation	802.3ad passive and 802.3ad active
Bridge Mode / Transparent Mode	Inspect traffic without interfering with the original IP routing
Extensive Set of Policy Objects	Individual node, networks, groups, dynamic objects
IP Versions	IPv4 and IPv6
Fail-Safe Protections	Default filter provides protection during boot time and prior to initial policy
Secure Internet Communications (SIC)	Certificate-based secure communications channel among all Check Point distributed components belonging to a single management domain

Authentication	
Multiple Authentication Methods	User authentication, client authentication, session authentication
Local Users	Local database user store included
RADIUS and RADIUS Groups	Multiple servers and MS-CHAPv2, MS-PAP methods
LDAP and LDAP Groups	Microsoft Active Directory, Novell Directory Server, Red Hat Directory Server, OPSEC certified LDAP server
TACACS+	Supported
RSA SecurID	Supported
X.509 Certificates	Supported using the included Certificate Authority or third party CAs
Customizable Authentication Messages	Supported

Para finalizar se muestra un gráfico de la consola de gestión de políticas del cortafuegos y la consola de logs:





En el escenario actual, se desplegará el Check Point Firewall Software Blade en un servidor HP ML 370 G6, que se trata de un servidor más potente que los anteriores descritos. Las características se pueden encontrar en *[16]*:

Especificaciones técnicas	
Procesador	Intel® Xeon® E5620 (4 núcleos, 2,40 GHz, 12 MB L3, 80 W)
Número de procesadores	1
Núcleo de procesador disponible	4
Memoria, estándar	4 GB
Ranuras de memoria	18 ranuras DIMM
Tipo de memoria	PC3-10600 DDR3-1333 registrado
Ranuras de expansión	9
Controlador de red	(1) 4 puertos 1 GbE NC375i multifunción
Tipo de fuente de alimentación	(1) 460 W CS alta eficacia
Controlador de almacenamiento	(1) Smart Array P410i/256 MB
Software de gestión	N/D
Tipo de unidad óptica	DVD ROM (SATA)
Formato (totalmente configurado)	4U
Garantía - año(s) (partes/mano de obra/in situ)	3/3/3

Alternativas

StoneGate de Stonesoft (ya expuesto en el punto de "Firewall Externo")

Servidor de monitorización

Solución de mercado elegida

Nagios (SW libre en Linux)

Nagios es un sistema de monitorización de equipos y de servicios de red, creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren antes de que los usuarios de la misma los perciban.

Como mencionan en *[25]*, se trata de un software usado en todo el mundo que debe correr en sistemas Linux o Unix y que permite extender su funcionalidad con la utilización o creación de extensiones. Está liberado bajo licencia GPL por lo que no está sometido a costes de licenciamiento.

Nagios es un sistema de monitorización muy completo, con grandes posibilidades de ampliación y adaptación como demuestra su implantación en empresas, universidades y organismos gubernamentales. Sin embargo, se trata de un sistema complejo que requiere una configuración e instalación elaborada que no lo hacen apropiado para ser usado en redes pequeñas.

Nagios es una solución robusta, escalable y económica para la monitorización de equipos y redes informáticas.

CARACTERÍSTICAS

Nagios, básicamente es un sistema que testea servicios y otros parámetros de una red, de muy diversas formas, y notifica todas las incidencias rápidamente a los administradores, es por tanto un *sistema de alerta temprana*.

Interfaz web: muestra la información en una interfaz web desde la que el propio administrador puede establecer algunos parámetros, lo que permite observar este interfaz de forma remota vía cliente HTTP. Incluso desde dicha interfaz web, previa autenticación HTTP, permite también programar en el tiempo los chequeos a máquinas o servicios previamente configurados, las notificaciones, etc.

Definición de jerarquías de servicios o de máquinas: Incorpora características muy interesantes como las dependencias de servicios o de equipos que permiten establecer jerarquías de servicios o de máquinas. De esta forma Nagios puede detectar si un servicio está inactivo o inaccesible; en el primer caso el equipo o servicio estaría down, mientras que en el segundo caso, el estado del servicio o equipo no se sabría porque la caída de uno superior impide su monitorización.

Administración y definición de usuarios: otra característica que ofrece es la agrupación de contactos (personas a quién notificar) de manera que cuando una incidencia se produzca para equipos o servicios supervisados por esas personas, dicha notificación llegue a todas y cada una de ellas y no exclusivamente a una persona. Esto proporciona flexibilidad si por ejemplo la administración de la red se realiza en jornadas divididas por turnos. De esta forma se puede hacer que se notifique solo a la persona que se encuentra en su jornada laboral o que se notifique a un grupo de personas.

Creación de nuevos comandos (plugins): Nagios también permite la creación sencilla de nuevos comandos (llamados plugins) para añadir nuevas

funcionalidades al sistema, o bien combinar varios de los que se encuentran activos. En cierto modo Nagios puede ser tan flexible como se desee tanto en cuanto es software libre y por tanto el código fuente es abierto y modificable por cualquiera.

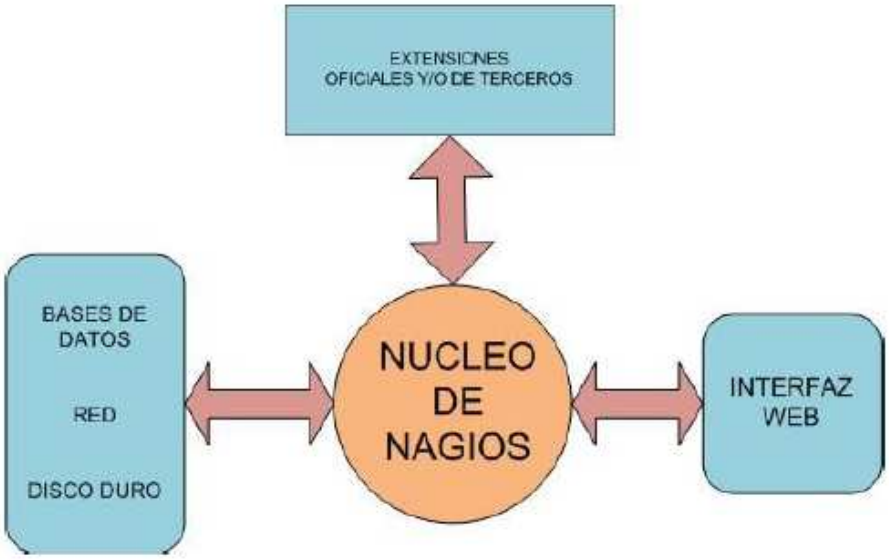
ESTRUCTURA

El núcleo de la aplicación, que forma la lógica de control de la aplicación, contiene el software necesario para realizar la monitorización de los servicios y equipos de la red que han sido definidos. Hace uso de diversos componentes que vienen con la aplicación, y puede hacer uso de otros componentes realizados por terceras personas.

Aunque permite la captura de paquetes SNMP para notificar sucesos, no es un sistema de monitorización y gestión basado en SNMP sino que realiza su labor basándose en una gran cantidad de pequeños módulos software que realizan chequeos de parte de la red.

Muestra los resultados de la monitorización y del uso de los diversos componentes en una interfaz web a través de un conjunto de CGI's y páginas HTML que vienen incorporadas de serie. Y que permiten al administrador una completa visión de qué ocurre, dónde y en algunos casos, el por qué.

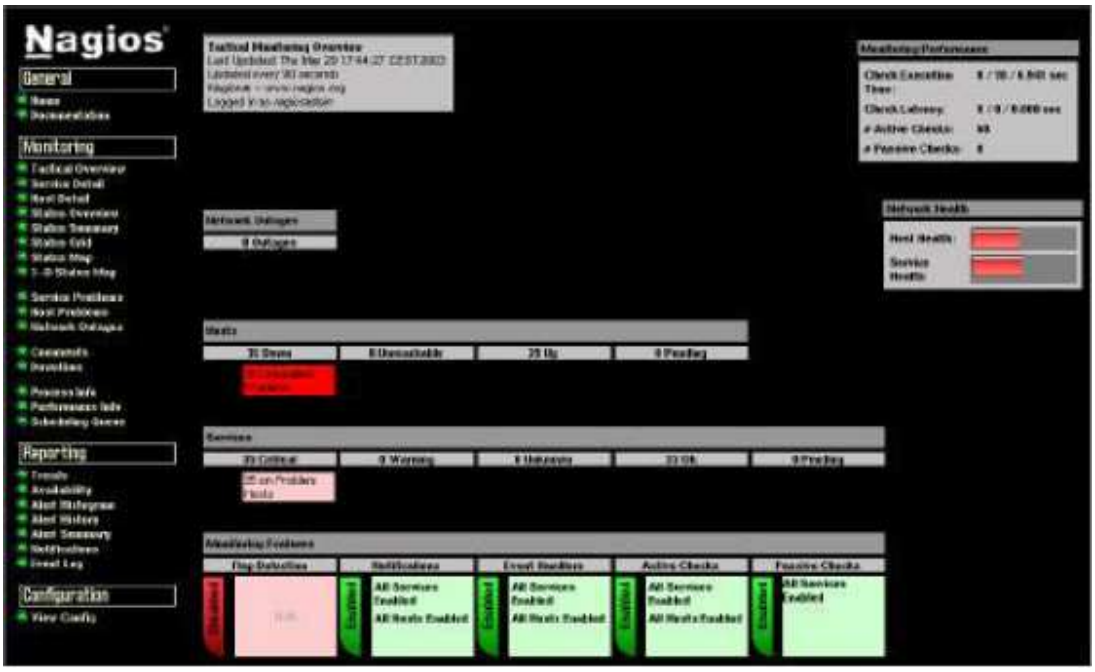
Por último, si se compila para ello, Nagios guardará los históricos en una base de datos para que al detener y reanudar el servicio de monitorización, todos los datos sigan como iban, sin cambios.



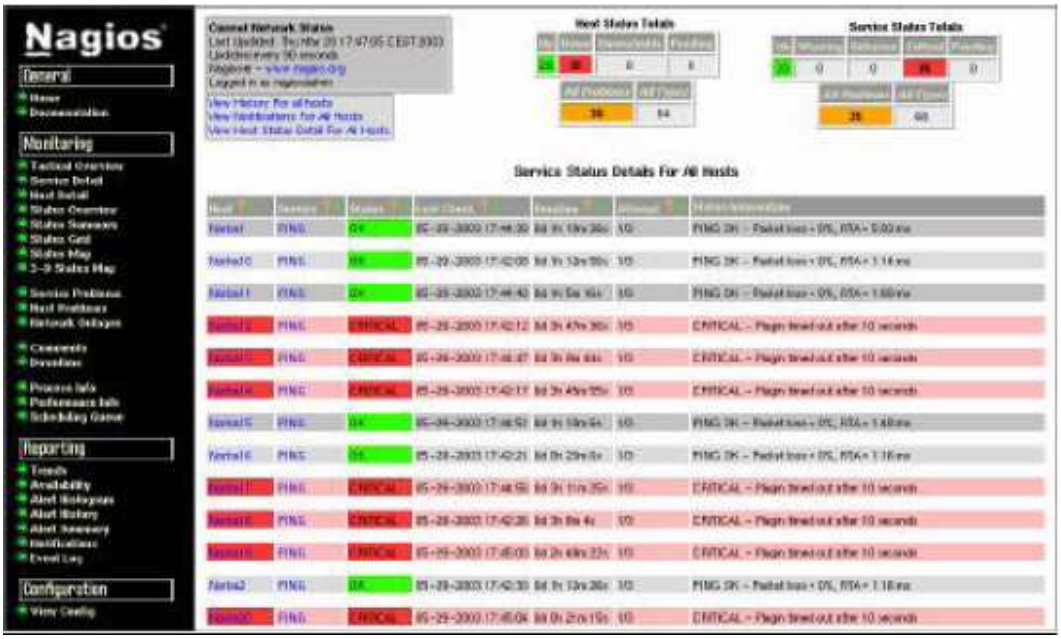
INTERFAZ WEB

La Web de administración de Nagios es altamente configurable, además existen numerosos plugins para hacer que se adapte a las necesidades particulares.

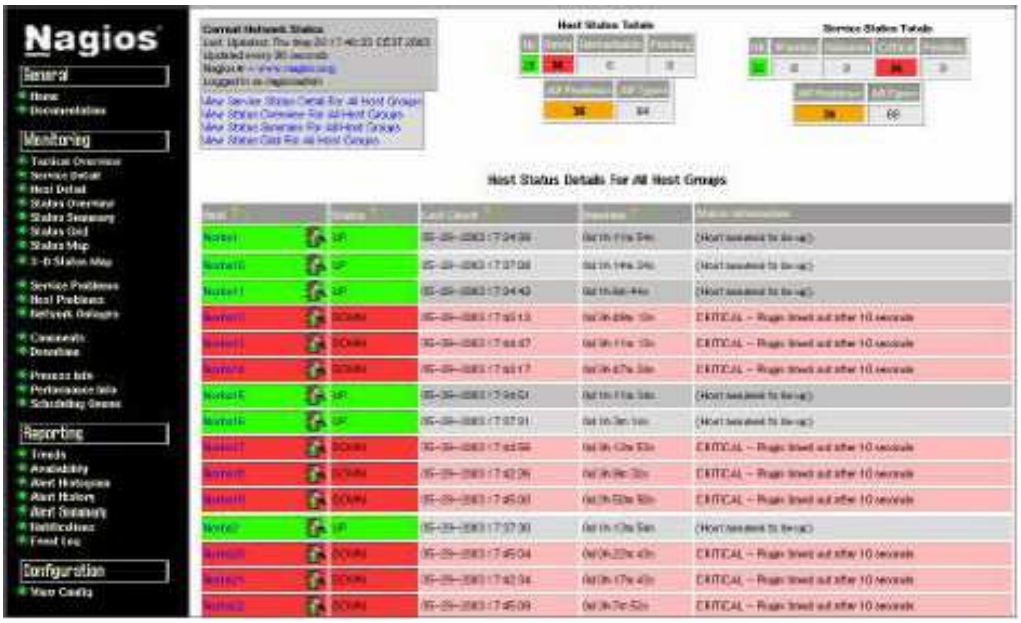
Visión general: Muestra de forma rápida un resumen de todo el sistema que permita tomar decisiones rápidas apoyadas en una base real del estado del sistema.



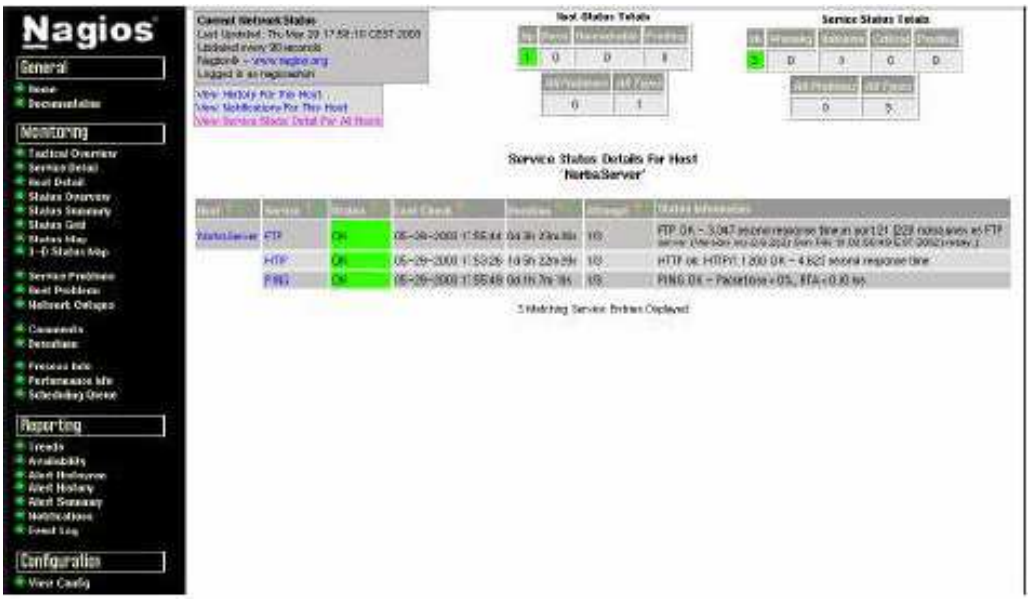
Detalle de los servicios: Muestra el estado de los servicios que se están monitorizando así como una descripción textual de si ha habido problemas, si no se tienen datos suficientes, etc.



Detalle de los equipos: Muestra si los equipos que están siendo monitorizados se encuentran activos, si se encuentran caídos o si el acceso a los mismos está dificultado por alguna cuestión.



Estado detallado de un equipo: Muestra para cada equipo monitorizado, su estado, el estado de los servicios que tiene asociados y algunos datos extra.

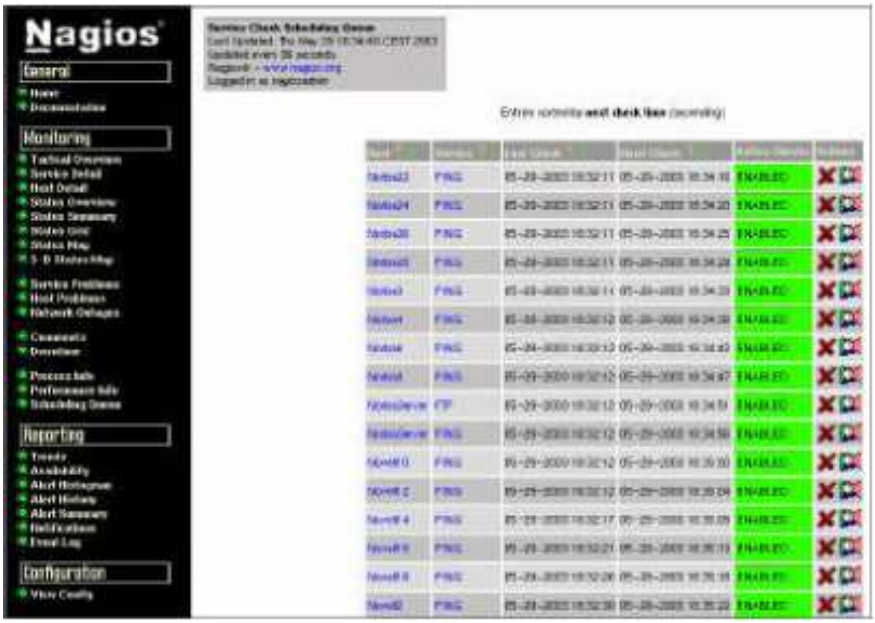


Información sobre un equipo: Muestra datos muy detallados sobre un equipo concreto y permite además la ejecución de algunos comandos que afectan a dicho equipo.

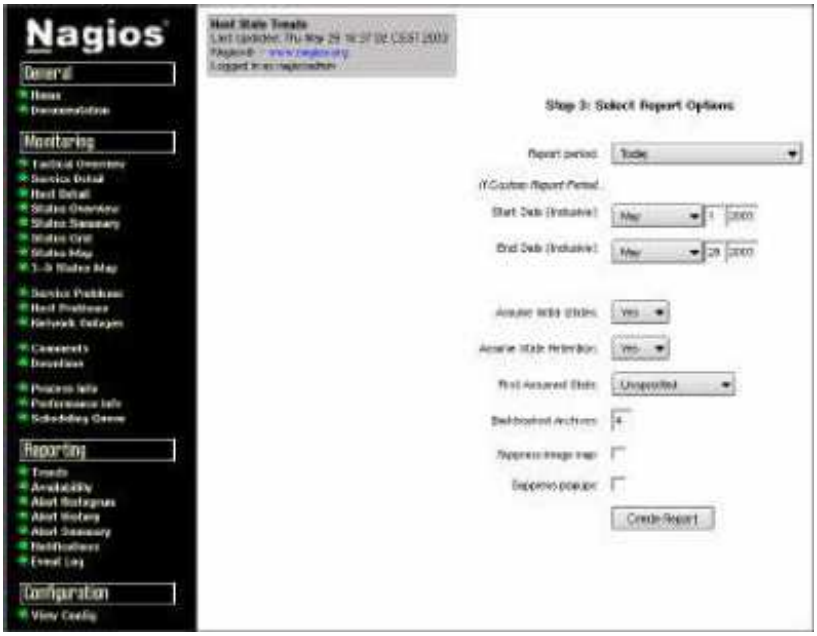
Problemas con los equipos: Esta opción muestra exclusivamente los equipos que están teniendo problemas así como una descripción de los mismos. Es especialmente útil para un administrador de red saber inmediatamente qué equipos están fallando.

Problemas con los servicios: Esta opción muestra exclusivamente los servicios que están teniendo problemas así como una descripción de dichos problemas. Es especialmente útil para un administrador de red saber inmediatamente qué servicios están dejando de funcionar.

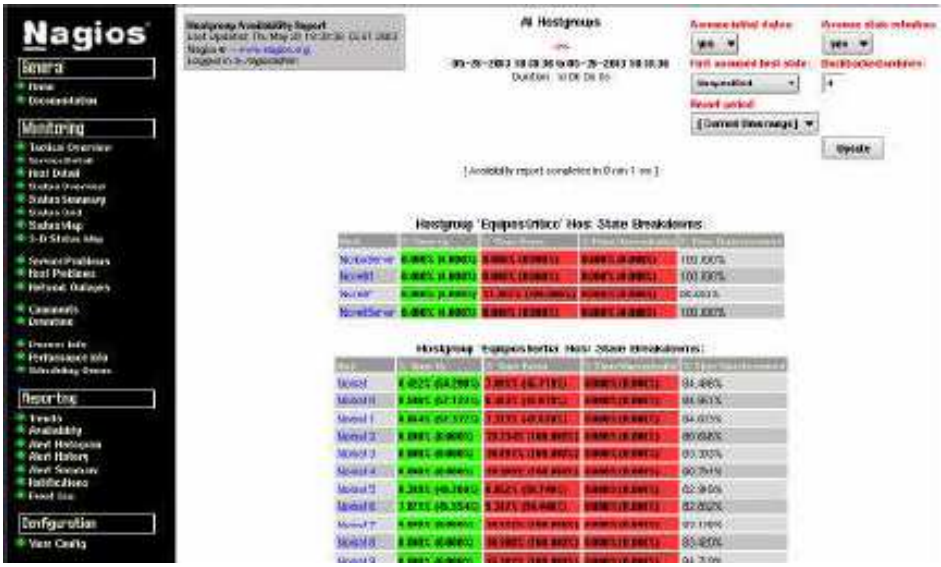
Cola de planificación: Esta opción muestra y permite cambiar la fecha y hora para la cual están planificadas la ejecución de los chequeos a servicios y equipos.



Configuración de informes: Común para casi cualquier informe. Permite elegir el rango de tiempo, la forma de presentación, el orden, etcétera, de los datos que aparecerán en el informe.

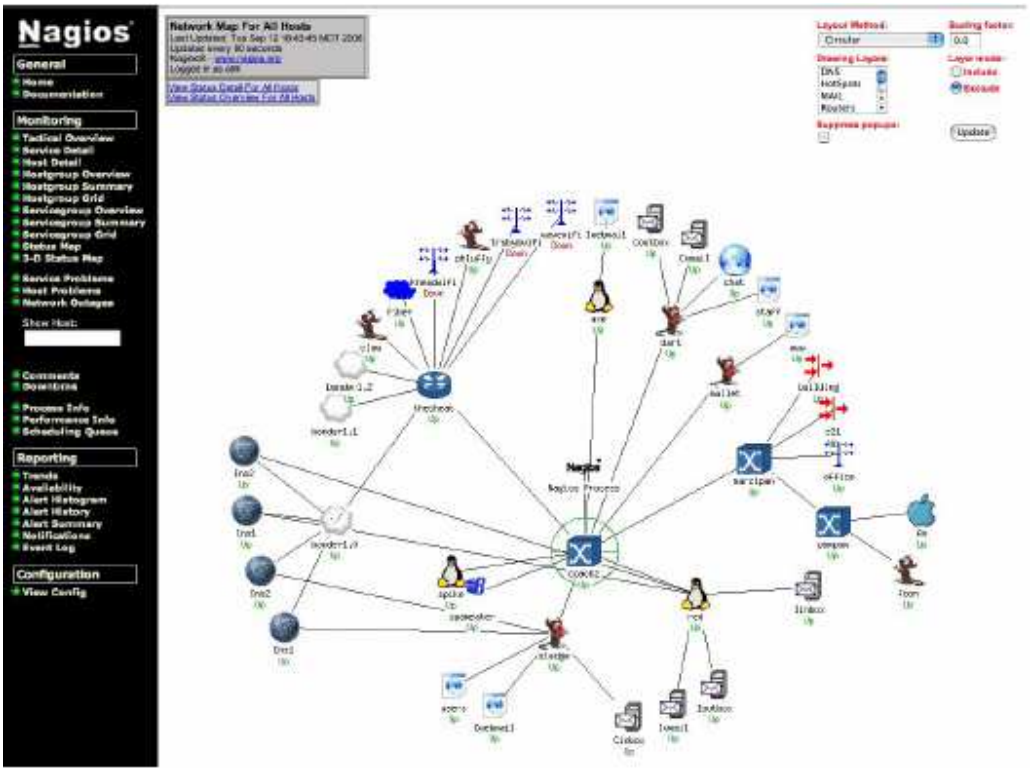


Informe de disponibilidad: Esta opción presenta en la ventana web un listado con todos los equipos y los porcentajes de tiempo en los que cada uno ha estado activo e inactivo. Esto permite obtener unas estadísticas para ver si una máquina falla con frecuencia y tomar medidas al respecto.



Histórico de eventos: Esta opción muestra el total de sucesos que han ocurrido en el sistema, desde la caída de un equipo hasta el envío a un contacto de una notificación vía correo electrónico.

Mapa: Esta opción permite ver un esquema gráfico de la red que monitoriza Nagios y el estado de cada elemento de la red:



El servidor de monitorización Nagios se instalará sobre un servidor HP DL 120 G7, ya que cubre todas las necesidades del servicio.

Características

A continuación se muestran las principales características del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Core™ i3 2100 (2 núcleos, 3,1 GHz, 3 MB, 65 W, 1333/t)
Número de procesadores	1
Núcleo de procesador disponible	2
Memoria, estándar	2 GB
Ranuras de memoria	4 ranuras DIMM
Tipo de memoria	PC3-10600E DDR3 UDIMMs
Ranuras de expansión	2
Controlador de red	(2) 1 puerto NC112i 1 GbE
Tipo de fuente de alimentación	(1) detección automática de 400 W, cumple con la marca CE
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	Ningún estándar de suministro
Formato (totalmente configurado)	1U
Garantía - año(s) (partes/mano de obra/in situ)	1/1/1

Alternativas

SolarWinds Application Performance Monitor

Tal y como indican en *[26]*, SolarWinds Application Performance Monitor (APM) ofrece una potente herramienta de monitorización, alertas y generación de informes de aplicaciones y servidores a un precio realmente asequible. En menos de una hora, APM puede descubrir sus aplicaciones y ofrecer la visibilidad que necesite en el rendimiento de las aplicaciones y los sistemas operativos que se ejecuten en determinados equipos.

Todo esto se provee sin necesidad de instalar agentes de ningún tipo en el servidor a monitorizar, siendo así fácil y rápido de implementar. Sólo se tiene que instalar el software en el servidor principal y seleccionar las aplicaciones y los servidores que desea supervisar.

CARACTERÍSTICAS

- Obtiene en un vistazo la visión del estado de las aplicaciones tanto en servidores virtuales como físicos de toda la infraestructura, todo a través de una única ventana. Es capaz de monitorizar casi cualquier aplicación que pueda correr en una máquina.

- Vigila en arquitecturas complejas de varios niveles de aplicación que son únicos en una determinada organización o entornos de IT mediante la agrupación de servidores y aplicaciones por servicio, localización o por departamento.

- Realiza análisis causa-raíz, a través de las aplicaciones y servidores del entorno.

- Detecta rápidamente la fuente de los problemas de rendimiento con una interfaz intuitiva, LUCID ™ diseñada para trabajar de la forma que prefieras.

- Tener control sobre cómo se le avisa mediante la configuración de alertas y secuencias de escalado en base a eventos correlacionados, condiciones repetidas, combinaciones complejas de estados, y muchos otros.

- Elimina las interrupciones innecesarias mediante la configuración de alertas inteligentes que reconocen dependencias de la aplicación y el servidor.

- Simula el comportamiento de los usuarios finales para determinadas aplicaciones más comunes, como puedan ser el HHTP o Mail.

- Se despliega de forma fácil y sencilla, y en menos de una hora ya se pueden obtener resultados con su potente motor de descubrimiento de aplicaciones.

- Se puede migrar de soluciones de código abierto como Nagios con los "Open Source Script Monitors".

- Se pueden utilizar los grupos y cuentas de usuario de Microsoft Active Directory para simplificar la creación de credenciales de acceso de Orión.

- Puede correr de manera autónoma SolarWinds APM o junto con Orion Network Performance Monitor (NPM) para una visión completa del rendimiento de aplicaciones, servidores y redes.

A continuación, sacado de *[26]*, se muestran las características físicas mínimas del hardware donde deberá correr el software APM:

Hardware	Minimum Requirenments
CPU	Dual Processor, 3GHz
Memory	3 GB
Hard Drive	20 GB
Software	Minimum Requirements
Operating System	Windows 2003 or Windows 2008R2 Server with IIS installed, running in 32-bit mode
.Net Framework	Version 3.5 or later
Database	SQL Server 2005 SP1 Express, Standard, or EnterpriseSQL Server 2008 (including R2) Express, Standard, or Enterprise

MONITORIZACIONES ESTANDARIZADAS

Sistemas operativos

- Microsoft Windows™ Server 2003 and 2008
- IBM AIX®
- HP-UX
- Linux® (Red Hat®, SuSE®, Ubuntu®) – SSH compatibility required
- Sun Solaris™
- UNIX

Servidores Web y monitores de URL

- HTTP User Experience
- HTTPS User Experience
- Microsoft® Internet Information Services (IIS)
- Apache®

Servidores de Mail y de Directorio

- Microsoft® Exchange 2000, 2003, 2007, & 2010 (Exchange Server)
- Microsoft Active Directory®
- Lotus Domino Servers
- BlackBerry Enterprise Server
- BlackBerry Delivery Confirmation
- LDAP and DHCP user experience monitors

Bases de Datos

- SQL Query User Experience
- Microsoft SQL Server®
- Oracle®
- MySQL
- ODBC User Experience
- Oracle User Experience

Servicios de Red

- DNS Query User Experience
- DNS Port
- SNMP, SMTP, TCP Port
- IMAP4
- POP3
- NNTP
- FTP User Experience
- Cisco Call Manager

Protocolos de seguridad

- RADIUS User Experience
- TACACS+ User Experience

De carácter General

- DNS Query User Experience
- WMI Performance Counter
- Windows® Script
- Linux Script
- Unix Script
- Windows Service
- Process Monitor (Windows, Linux, Unix)
- File and Directory
- Nagios® Script
- Windows Event Log
- Windows Printer
- Microsoft SharePoint®
- Citrix XenApp
- Dell® Servers

MONITORIZACIONES PERSONALIZADAS

Monitores Virtuales

- Microsoft Hyper-V™
- VMware® (ESX Server)

Servidores de Aplicación

- Microsoft .NET™ Server
- Java™ 2 Platform, Enterprise Edition Server (J2EE)
- Apache Tomcat™

- Apache Geronimo™
- Oracle® E-Business Suite
- IBM WebSphere®
- SAP R/3™
- SAP NetWeaver™
- WebLogic

Servidores de Backup

- Symantec Backup Exec™
- Symantec NetBackup™
- Microsoft Data Protection Manager

Ya que SolarWinds necesita unos requisitos hardware mayores a Nagios, se utilizará un servidor HP ML 330 G6.

A continuación se muestran las características más importantes del servidor *[16]*:

Especificaciones técnicas	
Procesador	Intel® Xeon® E5606 (4 núcleos, 2,13 GHz, 12 MB L3, 80 W)
Número de procesadores	1
Núcleo de procesador disponible	4
Memoria, estándar	4 GB
Ranuras de memoria	12 ranuras DIMM
Tipo de memoria	PC3-10600E (UDIMM)
Ranuras de expansión	(4) ranuras PCI-E y (2) ranuras PCI-X opcionales, con ampliador PCI X (usa 1 ranura PCI-E)
Controlador de red	(1) 2 Puertos 1 GbE NC326i
Descripción de unidad	(8) SAS/SATA LFF; sin conexión en caliente o conexión en caliente
Tipo de fuente de alimentación	(1) 460 W sin conexión en caliente, no redundante
Controlador de almacenamiento	(1) Smart Array B110i SATA RAID
Software de gestión	N/D
Tipo de unidad óptica	DVD-ROM SATA media altura
Formato (totalmente configurado)	Bastidor de 5U, torre
Garantía - año(s) (partes/mano de obra/in situ)	3/1/1

5.3 Banco de pruebas

Se han definido los siguientes bloques funcionales para la realización de las pruebas:

- Grupo de Bloques orientados a servicios críticos:
  - Bloque de Navegación (A)
  - Bloque de Correo (B)

- Grupo de Bloques orientados a sistemas críticos:
  - Bloque de cortafuegos interno (1)
  - Bloque de cortafuegos externo (2)
  - Bloque de gestión de ancho de banda (3)
  - Bloque de Radius (4)
  - Bloque de DNS (5)
  - Bloque de IDS de Red (6)
  - Bloque de Antivirus Web (7)
  - Bloque de Antivirus de Correo (8)
  - Bloque de Proxy (9)
  - Bloque de Servidor de monitorización (10)

PRUEBAS ORIENTADAS A SERVICIOS CRÍTICOS

BLOQUE A

El bloque A se corresponde con el servicio de NAVEGACIÓN.

CASO DE PRUEBA A-001

Descripción: Acceso a Internet desde la red interna con Proxy

Configuración de la prueba: Se comprueba el acceso a Internet desde la LAN interna a través del proxy y el antivirus.

Resultado esperado: Se navega correctamente.

Resultado obtenido: Ok.

BLOQUE B

El bloque B se corresponde con el servicio de CORREO.

CASO DE PRUEBA B-001

Descripción: Envío y recepción de correos a direcciones externas.

Configuración de la prueba: Se envía un correo desde una dirección interna a una dirección externa y se responde al correo.

Resultado esperado: Se reciben ambos correos.

Resultado obtenido: Ok.

PRUEBAS ORIENTADAS A SISTEMAS CRÍTICOS

BLOQUE 1

El bloque 1 corresponde al CORTAFUEGOS INTERNO (CHECKPOINT).

CASO DE PRUEBA 1-001

Descripción: Verificación del cluster.

Configuración de la prueba: Se verifica el cluster desde la interfaz gráfica.

Resultado esperado: Cluster XL está activado y funcionando en modo load sharing.

Resultado obtenido: Ok.

CASO DE PRUEBA 1-002

Descripción: Comprobación de la política de seguridad instalada.

Configuración de la prueba: Se verifica que existe una política de seguridad instalada.

Resultado esperado: Existe una política de seguridad aplicada al cluster de cortafuegos. Dicha política se almacena en el equipo management de la red de gestión.

Resultado obtenido: Ok.

CASO DE PRUEBA 1-003

Descripción: Conectividad con Management.

Configuración de la prueba: Se verifica la conectividad con el equipo Management.

Resultado esperado: Desde el equipo Management se aplica con éxito una política al cluster de cortafuegos interno.

Resultado obtenido: Ok.

CASO DE PRUEBA 1-004

Descripción: Configuración de redes.

Configuración de la prueba: Se verifica la configuración de las redes del cortafuegos.

Resultado esperado: Desde la consola de administración se verifica en las propiedades del cluster que se han configurado las distintas redes.

Resultado obtenido: Ok.

CASO DE PRUEBA 1-005

Descripción: Configuración de interfaces de red.

Configuración de la prueba: Se verifica la velocidad de cada interfaz.

Resultado esperado: Desde línea de comandos y con el comando eth_set se verifica que los interfaces gigabit están funcionando a 1000 full-duplex.

Resultado obtenido: Ok

CASO DE PRUEBA 1-006

Descripción: Reglas de acceso.

Configuración de la prueba: Se verifican las reglas de seguridad del cluster de firewalls interno.

Resultado esperado: Se limita el acceso directo a Internet desde la red interna salvo casos excepcionales. Se limita el tráfico entre las distintas redes conectadas al cortafuegos interno salvo las estrictamente necesarias.

Resultado obtenido: Ok.

CASO DE PRUEBA 1-007

Descripción: Activación de logs de tráfico.

Configuración de la prueba: Se verifica que se han activado los logs en las reglas del cluster.

Resultado esperado: Cada regla tiene activada la opción de guardar logs, salvo las específicamente creadas para evitar el almacenamiento masivo de logs como el caso de netbios.
Resultado obtenido: Ok.

CASO DE PRUEBA 1-008

Descripción: Rotación de logs.
Configuración de la prueba: Se verifica que hay una política de rotación de logs.
Resultado esperado: Desde la interfaz gráfica se accede a las propiedades del cluster y se comprueba que existe una política de rotación de logs.
Resultado obtenido: Ok.

CASO DE PRUEBA 1-009

Descripción: Backup de configuración.
Configuración de la prueba: Se verificará que existe un procedimiento de backup de la configuración.
Resultado esperado: Existe un procedimiento de backup periódico, manual o automático, de la configuración en el equipo Management.
Resultado obtenido: Ok.

BLOQUE 2

El bloque 2 corresponde al CORTAFUEGOS EXTERNO (STONEGATE).

CASO DE PRUEBA 2-001

Descripción: Comprobación de la configuración del cluster en modo HA con balanceo de carga.
Configuración de la prueba: Se verifica el estado desde la interfaz gráfica.

Resultado esperado: El estado de los dos nodos es online, lo que indica que están configurados en modo HA con balanceo de carga.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-002

Descripción: Conectividad con SMC.
Configuración de la prueba: Se verifica la conectividad de los nodos del cortafuegos con el equipo SMC.
Resultado esperado: Desde el equipo SMC se aplica con éxito una política a los cortafuegos.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-003

Descripción: Comprobación de la política de seguridad instalada.
Configuración de la prueba: Se verifica desde la interfaz gráfica que existe una política de seguridad instalada.
Resultado esperado: Existe una política de seguridad aplicada al cluster de cortafuegos. Dicha política se almacena en el equipo SMC de la red de gestión.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-004

Descripción: Configuración de redes.
Configuración de la prueba: Se verifica la configuración de las redes del cortafuegos.
Resultado esperado: Desde la consola de administración se verifica en las propiedades del cluster que se han configurado las distintas redes.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-005

Descripción: Configuración de interfaces de red.

Configuración de la prueba: Se verifica la velocidad de cada interfaz.

Resultado esperado: Desde línea de comandos y con el comando ethtool se verifica que todos los interfaces están funcionando a 1000 full-duplex.

Resultado obtenido: Ok.

CASO DE PRUEBA 2-006

Descripción: Acceso a Internet restringido.

Configuración de la prueba: Se verifica en las reglas del cluster externo el acceso a internet.

Resultado esperado: Ningún equipo podrá acceder directamente a Internet salvo en casos particulares como los proxies de navegación por http, los frontales de correo por smtp o los servidores de nombres por dns.

Resultado obtenido: Ok.

CASO DE PRUEBA 2-007

Descripción: Activación de logs de tráfico.

Configuración de la prueba: Se verifica que se han activado los logs en las reglas del cluster.

Resultado esperado: Cada regla tiene activada la opción de guardar logs, salvo las específicamente creadas para evitar el almacenamiento masivo de logs como.

Resultado obtenido: Ok.

CASO DE PRUEBA 2-008

Descripción: Rotación de logs.

Configuración de la prueba: Se verifica que hay una política de rotación de logs.

Resultado esperado: Desde la interfaz gráfica se accede a log data tasks y se comprueba que existe una política de rotación de logs.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-009

Descripción: Comprobación de licencia para VPN.
Configuración de la prueba: Desde la interfaz gráfica se comprueban los detalles de la licencia instalada.
Resultado esperado: La licencia instalada soporta la configuración de VPNs.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-010

Descripción: Reglas de NAT hacia el exterior.
Configuración de la prueba: Desde la interfaz gráfica se accede a las reglas de NAT.
Resultado esperado: Existirán reglas de NAT estático para el acceso a servidores de la DMZ desde Internet. También existirán reglas de NAT dinámico para la salida a Internet desde las redes internas.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-011

Descripción: Backup de configuración programado.
Configuración de la prueba: Se verifican las tareas programadas.
Resultado esperado: Existe una tarea semanal que consiste en realizar una copia de seguridad de la configuración.
Resultado obtenido: Ok.

CASO DE PRUEBA 2-012

Descripción: Prueba de HA en routers de salida a internet.

Configuración de la prueba: Se desconecta cada switch que conecta con el router de salida a Internet por separado y se prueba la navegación.

Resultado esperado: Sigue habiendo salida a Internet después de cada desconexión.

Resultado obtenido: Ok.

CASO DE PRUEBA 2-013

Descripción: Prueba de alta disponibilidad del cortafuegos externo.

Configuración de la prueba: Se apaga uno de los nodos. Ejecución de ping continuo desde un portátil situado en la red de gestión, hacia Internet (Google).

Resultado esperado: No deben apreciarse retrasos en las respuestas.

Resultado obtenido: Ok.

BLOQUE 3

El bloque 3 corresponde al GESTOR DE ANCHO DE BANDA (ALLOT).

CASO DE PRUEBA 3-001

Descripción: Prueba de flujo de tráfico a través de sus interfaces.

Configuración de la prueba: Se comprueba y monitoriza tráfico desde la interfaz web.

Resultado esperado: Desde la interfaz web se obtienen gráficas del tráfico en tiempo real.

Resultado obtenido: Ok.

CASO DE PRUEBA 3-002

Descripción: Limitación de tráfico.

Configuración de la prueba: Se inicia una descarga por FTP de un fichero de gran tamaño y se limita el ancho de banda durante la descarga.

Resultado esperado: Al aplicar la limitación al FTP se observa que la velocidad de descarga disminuye visiblemente. Al deshabilitarla se recupera la velocidad original.

Resultado obtenido: Ok.

CASO DE PRUEBA 3-003

Descripción: Alta disponibilidad de fuentes de alimentación.

Configuración de la prueba: Una por una se desconectan las fuentes de alimentación.

Resultado esperado: Al tratarse de fuentes de alimentación redundadas, siempre que haya al menos una conectada, el appliance permanecerá activo.

Resultado obtenido: Ok.

CASO DE PRUEBA 3-004

Descripción: Desconexión total de la alimentación eléctrica.

Configuración de la prueba: Se desconectan los tres cables de alimentación para simular una caída del suministro eléctrico.

Resultado esperado: El tráfico no debe interrumpirse en ningún momento ya que en caso de caída del equipo, los interfaces de entrada y salida se puentean.

Resultado obtenido: Ok.

BLOQUE 4

El bloque 4 corresponde al Servidor radius.

CASO DE PRUEBA 4-001

Descripción: Autenticación de usuario creado.

Configuración de la prueba: Se realiza la conexión con un usuario existente creado en servidor radius.

Resultado esperado: El usuario se conecta de forma satisfactoria y se le asigna la IP esperada para dicho usuario

Resultado obtenido: Ok.

CASO DE PRUEBA 4-002

Descripción: Monitorización de conexiones.

Configuración de la prueba: Se realiza la conexión con un usuario correcto y con otro incorrecto

Resultado esperado: Se observa en los log la conexión correcta del usuario, con el tiempo de conexión, flujo de datos de conexión, etc. También se observa el intento de conexión del usuario incorrecto.

Resultado obtenido: Ok.

BLOQUE 5

El bloque 5 corresponde al DNS.

CASO DE PRUEBA 5-001

Descripción: Resolución de nombres externos.

Configuración de la prueba: Se comprobará la resolución de nombres de Internet desde las redes internas.

Resultado esperado: El DNS responderá las peticiones de dominios externos.
Resultado obtenido: Ok.

CASO DE PRUEBA 5-002

Descripción: Resolución de nombres de dominios publicados.
Configuración de la prueba: Se comprobará la resolución de nombres para los dominios publicados.
Resultado esperado: El DNS responderá las peticiones de dominios publicados por él.
Resultado obtenido: Ok.

CASO DE PRUEBA 5-003

Descripción: Resolución de nombres al exterior de dominios no publicados.
Configuración de la prueba: Se comprobará la resolución de nombres desde Internet para otros dominios externos.
Resultado esperado: Los servidores DNS no resolverán peticiones desde Internet de dominios que no publique.
Resultado obtenido: Ok.

CASO DE PRUEBA 5-004

Descripción: Backup de configuración.
Configuración de la prueba: Se verificará que existe un procedimiento de backup de la configuración.
Resultado esperado: Existe un procedimiento de backup periódico, manual o automático, de la configuración, en los servidores DNS.
Resultado obtenido: Ok.

BLOQUE 6

El bloque 6 corresponde al IDS DE RED (STONEGATE).

CASO DE PRUEBA 6-001

Descripción: Conectividad con Analyzer.

Configuración de la prueba: Se comprobará la conectividad con el equipo Analyzer.

Resultado esperado: Existe conectividad con el equipo Analyzer, desde cada una de las sondas y desde la management de StoneGate.

Resultado obtenido: Ok.

CASO DE PRUEBA 6-002

Descripción: Conectividad con SMC.

Configuración de la prueba: Se comprobará la conectividad con el equipo SMC, desde el que se lleva a cabo la gestión.

Resultado esperado: Existe conectividad con el equipo SMC.

Resultado obtenido: Ok.

CASO DE PRUEBA 6-003

Descripción: Captura de tráfico.

Configuración de la prueba: Se comprobará que se recibe tráfico de las redes monitorizadas.

Resultado esperado: Se recibe tráfico.

Resultado obtenido: Ok.

BLOQUE 7

El bloque 7 corresponde al ANTIVIRUS WEB.

CASO DE PRUEBA 7-001

Descripción: Análisis de archivos descargados.

Configuración de la prueba: Se descargan desde Internet ficheros infectados para comprobar que el antivirus los detecta por HTTP y FTP tanto normales como comprimidos.

Resultado esperado: El antivirus no deja pasar los virus descargados. Detecta los virus dentro de los zip.

Resultado obtenido: Ok.

CASO DE PRUEBA 7-002

Descripción: Comprobación de alta disponibilidad.

Configuración de la prueba: Se comprueba que están funcionando en alta disponibilidad desconectando cada uno de ellos por separado.

Resultado esperado: Después de cada desconexión, el servicio continúa siendo operativo.

Resultado obtenido: Ok.

CASO DE PRUEBA 7-003

Descripción: Comprobación de backup.

Configuración de la prueba: Se lleva a cabo un backup de la configuración.

Resultado esperado: Se genera un fichero .tgz con la configuración del sistema.

Resultado obtenido: Ok.

BLOQUE 8

El bloque 8 corresponde al ANTIVIRUS DE CORREO.

CASO DE PRUEBA 8-001

Descripción: Análisis de virus.

Configuración de la prueba: Se envía un correo con un adjunto ilegal.

Resultado esperado: El antivirus bloquea el adjunto.

Resultado obtenido: Ok.

CASO DE PRUEBA 8-002

Descripción: Función de relay de correo.

Configuración de la prueba: Se envía un correo desde un puesto cliente a una dirección de correo externa para comprobar que funcionan como relay de correo de los servidores internos.

Resultado esperado: El correo llega a su destino.

Resultado obtenido: Ok.

CASO DE PRUEBA 8-003

Descripción: Relay no permitido a direcciones externas.

Configuración de la prueba: Se envía un correo desde una dirección externa a otra dirección externa utilizando el servidor como relay.

Resultado esperado: El servidor debe devolver un error al cliente.

Resultado obtenido: Ok.

BLOQUE 9

El bloque 9 corresponde al PROXY.

CASO DE PRUEBA 9-001

Descripción: Navegación con proxy.

Configuración de la prueba: Se configura un navegador de la LAN interna con cada servidor proxy y se comprueba la navegación.

Resultado esperado: La navegación es correcta.

Resultado obtenido: Ok.

CASO DE PRUEBA 9-002

Descripción: Navegación con proxy a páginas no permitidas.

Configuración de la prueba: Se configura un navegador de la LAN interna con cada servidor proxy y se comprueba la navegación hacia sitios no permitidos en la política de bloqueos implementada.

Resultado esperado: Se deniega el acceso.

Resultado obtenido: Ok.

CASO DE PRUEBA 9-003

Descripción: Alta disponibilidad.

Configuración de la prueba: Se desconecta cada proxy por separado para comprobar la disponibilidad del sistema.

Resultado esperado: El servicio continúa operativo.

Resultado obtenido: Ok.

CASO DE PRUEBA 9-004

Descripción: Backup.

Configuración de la prueba: Se verificará que existe un procedimiento de backup de la configuración.

Resultado esperado: Existe un procedimiento de backup periódico, manual o automático, de la configuración.

Resultado obtenido: Ok.

BLOQUE 10

El bloque 10 corresponde al Servidor de monitorización de equipos (NAGIOS).

CASO DE PRUEBA 10-001

Descripción: Detección de servidor remoto caído.

Configuración de la prueba: Se apagar uno de los servidores que se monitoriza.

Resultado esperado: Todos los servicios monitorizados en ese servidor aparecen como caídos.

Resultado obtenido: Ok.

CASO DE PRUEBA 10-002

Descripción: Detección de servicio caído.

Configuración de la prueba: Se fuerza a apagar uno de los servicios que se están monitorizando en el servidor remoto.

Resultado esperado: Aparece una alerta en la consola de Nagios como que únicamente el servicio suspendido en el servidor remoto está caído.

Resultado obtenido: Ok.

CASO DE PRUEBA 10-003

Descripción: Recuperación de servidor monitorizado.

Configuración de la prueba: Se levanta el servidor remoto que se está monitorizando.

Resultado esperado: Todas las alertas del equipo monitorizado desaparecen y vuelven a estado correcto.

Resultado obtenido: Ok.

CASO DE PRUEBA 10-004

Descripción: Recuperación de servicio monitorizado.

Configuración de la prueba: Se levanta el servicio que se está monitorizando en el servidor remoto.

Resultado esperado: La alerta del servicio que estaba caído desaparece y aparece como en estado correcto.

Resultado obtenido: Ok.

5.4 Gestión de la infraestructura

Componente 1: Cortafuegos de primer nivel (StoneGate)

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Revisión de logs en busca de algún funcionamiento anómalo. • Verificación de la correcta rotación de logs • Resolución de incidencias, mantenimiento y soporte de la política de reglas. • Búsqueda de vulnerabilidades y fallos conocidos del sistema del sistema en listas de distribución y páginas web. • Instalación de parches críticos de seguridad publicados para vulnerabilidades críticas que afecten al sistema.
SEMANAL	• Búsqueda de nuevas versiones y mejoras de StoneGate. • Instalación de parches de funcionalidad y nuevas versiones publicadas para StoneGate. • Revisión del correcto funcionamiento del Log Server y consola de gestión del sistema cortafuegos StoneGate. • Verificación de la capacidad de disco para almacenar logs.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
MENSUAL	• Revisión general de la política de seguridad de los sistemas cortafuegos internos.

Tabla 1: Listado de tareas en los cortafuegos de primer nivel (StoneGate)

Componente 2: Cortafuegos de segundo nivel (CheckPoint)

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Revisión de logs en busca de algún funcionamiento anómalo. • Verificación de la correcta rotación de logs • Resolución de incidencias, mantenimiento y soporte de la política de reglas. • Búsqueda de vulnerabilidades y fallos conocidos del sistema del sistema en listas de distribución y páginas web. • Instalación de parches críticos de seguridad publicados para vulnerabilidades críticas que afecten al sistema.
SEMANAL	• Búsqueda de nuevas versiones y mejoras de CheckPoint. • Instalación de parches de funcionalidad y nuevas versiones publicadas por CheckPoint. • Verificación de la capacidad de disco para almacenar logs
MENSUAL	• Revisión general de la política de seguridad de los

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
	sistemas cortafuegos externos

Tabla 2: Listado de tareas en los cortafuegos de segundo nivel (CheckPoint)

Componente 3: Sondas de detección de intrusos (SiteProtector ISS y StoneGate IPS)

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Revisión de logs generados por las sondas de red. • Supervisión del espacio del disco para guardar los logs generados por las sondas de red y de host • Búsqueda de nuevas versiones de patrones de firmas para las sondas de red y de host. • Resolución de incidencias, mantenimiento y soporte de la política de las sondas de red.
SEMANAL	• Ajuste de las políticas de seguridad de las sondas para adaptarse al tráfico inspeccionado. • Verificación del correcto funcionamiento de las respuestas definidas en la política de reglas. • Instalación de parches de funcionalidad y nuevas versiones publicadas por ISS y StoneSoft.
MENSUAL	• Actualización y revisión de los distintos componentes de la consola de gestión SiteProtector de ISS y de la consola StoneSoft.

Tabla 3: Listado de tareas en los sistemas de detección de intrusos

Componente 4: Antivirus perimetral (Esafe)

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Revisión de logs generados por el antivirus perimetral • Verificación de la correcta actualización de las firmas del antivirus • Resolución de incidencias, mantenimiento y soporte de la política de reglas del antivirus. • Instalación de parches de seguridad publicados para vulnerabilidades críticas que afecten al sistema. • Revisión de las listas de distribución de los fabricantes de antivirus para conocer la aparición de nuevos virus
SEMANAL	• Búsqueda de nuevas versiones del producto • Rotación de logs del antivirus y supervisión del espacio del disco para guardar los logs generados por las sondas
MENSUAL	• Obtención, a través de la herramienta (Esafe), de un informe con el número de correos escaneados.

Tabla 4: Listado de tareas en los sistemas de antivirus perimetral (Esafe)

Componente 5: Gestor de ancho de banda

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Resolución de incidencias, mantenimiento y soporte del gestor de ancho de banda.
SEMANAL	• Revisión de la aparición de nuevas versiones y actualizaciones del gestor de ancho de banda.
MENSUAL	• Revisión de logs generados por el gestor de ancho de banda • Adaptación de las políticas de seguridad del gestor de ancho de banda para adaptarse al tráfico de la organización.

Tabla 5: Listado de tareas en el gestor de ancho de banda

Componente 6: Servidores DNS

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Comprobar que se accede desde el exterior (Internet) al servicio de DNS, tanto al servidor primario como al secundario.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
	• Revisar el registro (logs) en busca de entradas anómalas. • En caso de existir otro servidor (ubicado fuera de la infraestructura de la organización), comprobar que está operativo. • Instalación de parches críticos de seguridad publicados para vulnerabilidades críticas que afecten al sistema.
SEMANAL	• Realizar un backup de la configuración de DNS de ambos servidores. • Comprobar mediante una consulta que los servidores de DNS primario y secundario siguen siendo los autoritativos para el dominio de la organización (si hubiera otro servidor ubicado fuera de la infraestructura, comprobad este servidor también). Si no fuera así, resultaría indicativo de que alguien ha cambiado la configuración de DNS a nivel organizativo.
MENSUAL	• Comprobar, viendo las diferencias con una copia de seguridad de que se disponga, de que la configuración de DNS no ha cambiado. Si ha cambiado, comprobar si ese cambio ha sido autorizado.

Tabla 6: Listado de tareas en los servidores DNS

Componente 7: Servidores NTP

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Comprobar que los dos servidores de NTP se están sincronizando con los servidores de tiempo externos. • Comprobar que los clientes internos pueden llegar a los servidores de NTP. • Revisar el registro (logs) en busca de entradas anómalas. • Atender las peticiones de cambio en la configuración de NTP. • Instalación de actualizaciones de software y/o parches críticos de seguridad publicados para vulnerabilidades críticas que afecten al sistema.
SEMANAL	• Realizar un backup de la configuración de NTP de ambos servidores.
MENSUAL	• Comprobar, viendo las diferencias con una copia de seguridad de que se disponga, de que la configuración de NTP no ha cambiado. Si ha cambiado, preguntarse si ese cambio ha sido no autorizado.

Tabla 7: Listado de tareas en los servidores NTP

Componente 8: Servidores de Correo (Esafe)

A continuación se expone, para este componente, el listado de tareas propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Comprobar que ambos servidores responden a peticiones en el puerto 25 (SMTP). • Comprobar que llegan correos desde el exterior dirigidos al dominio de la organización. • Comprobar que el sistema de balanceo está funcionando. • Atender las peticiones de cambio en la configuración del relay. • Instalación de actualizaciones de software y/o parches críticos de seguridad publicados para vulnerabilidades críticas que afecten al sistema.
SEMANAL	• Realizar un backup de la configuración de los servidores de correo. • Revisar el registro (logs) en busca de entradas anómalas. • Comprobar que no puede utilizarse la pasarela de correo como relay para enviar correo (desde Internet) a dominios diferentes al de la organización
MENSUAL	• Comprobar, viendo las diferencias con una copia de

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
	seguridad de que se disponga, de que la configuración de RELAY de correo no ha cambiado.

Tabla8: Listado de tareas en los servidores de correo

Componente 9: Servidores Proxy (SQUID)

A continuación se expone, para este componente, el listado de tareas de gestión operativa propuestas y su periodicidad.

PERIODICIDAD	DESCRIPCIÓN DE TAREAS
DIARIA	• Verificación de la capacidad de CPU en horas punta. • Verificación de la capacidad de disco para almacenar los logs generados. • Instalación de parches de seguridad publicados para vulnerabilidades críticas que afecten al sistema. • Resolución de incidencias, mantenimiento y soporte de Squid.
SEMANAL	• Búsqueda de nuevas versiones del producto.
MENSUAL	• Instalación de parches de funcionalidad y nuevas versiones publicadas para Squid.

Tabla9: Listado de tareas de los servidores proxy

5.5 Metodología de gestión

A continuación se presenta una serie de ejemplos de actuación ante situaciones tipo dentro de la gestión operativa de la plataforma. Es importante recalcar que estos procedimientos han sido incluidos de forma resumida en esta propuesta a modo de sugerencias de actuación, estando sujetos a su revisión y análisis para adaptarlos a las necesidades del entorno de producción.

Procedimiento de actuación ante un fallo de un elemento de red

En este apartado se describe el procedimiento de actuación frente al fallo de un elemento de red de la infraestructura de seguridad perimetral.

Los pasos a seguir son los siguientes:

- Detección del fallo en la red, mediante el uso de los sistemas de gestión de las plataformas.
- Se clasificaría la incidencia según nivel de criticidad (alta, media, baja)
- En caso de criticidad alta (indisponibilidad de algún servicio esencial) se procedería a informar de forma inmediata al responsable de la organización.
- Se procederá a intentar resolver el problema.
- Si en un plazo razonable el problema persistiera se escalaría el problema al equipo de soporte del fabricante del elemento de red.
- Una vez resuelta la incidencia se documentaría su desarrollo y resolución.

Procedimiento de actuación ante la detección de una vulnerabilidad

En este apartado se describe el procedimiento de actuación frente a la detección de una vulnerabilidad en un elemento de red.

Los pasos a seguir son los siguientes:

- Detección de la vulnerabilidad, en el transcurso de una revisión periódica o mediante la notificación de una incidencia.
- Estudio y análisis de la vulnerabilidad (cuantificación de la amenaza y riesgo asociado a esa vulnerabilidad).
- En caso de vulnerabilidad grave con un alto índice de riesgo se procedería a informar de forma inmediata al responsable de la organización.
- Se procederá a buscar una solución a dicha vulnerabilidad.
- Una vez encontrada la forma de solucionar dicha vulnerabilidad se procederá a mitigarla (instalando parches, cerrando servicios, etc,). Si el sistema afectado no pertenece a la infraestructura de seguridad perimetral, se procedería a informar al administrador correspondiente de cómo mitigar la vulnerabilidad.
- Una vez resuelta la vulnerabilidad se documentaría su desarrollo y resolución en un informe de vulnerabilidad.

Procedimiento de actuación ante la detección de un ataque

En este apartado se describe el procedimiento de actuación frente a la detección de que un ataque ha sido llevado a cabo sobre un elemento de red de la infraestructura de seguridad perimetral.

Los pasos a seguir son los siguientes:

- Detección del ataque, en el transcurso de una revisión periódica o de un procedimiento de monitorización, o mediante la notificación de una incidencia.
- Estudio y análisis del ataque: elementos afectados, valoración de su éxito o fracaso, vulnerabilidades explotadas.
- En caso de ataque grave con éxito se procedería a informar de forma inmediata al responsable de la organización y, en caso necesario, a proceder al aislamiento del equipo o equipos afectados.
- En caso de ataque con éxito se procederá a evaluar las posibles soluciones que impidan la repetición del ataque, mediante la eliminación de la vulnerabilidad que hizo posible dicho ataque.
- En todos los casos se documentarían las características del ataque mediante un informe.

Procedimiento de actuación ante la realización de un cambio en la red

En este apartado se describe el procedimiento de actuación frente a la realización de un cambio en la red a llevar a cabo sobre un elemento de red de la infraestructura de seguridad perimetral.

Los pasos a seguir son los siguientes:

- Determinación del alcance del cambio, elementos afectados, implicaciones del cambio y duración del procedimiento de cambio (migración).
- Elaboración de un plan de cambio de red (o plan de migración).
- Autorización del cambio por parte de la organización.
- Programación del cambio en horario de mínimo impacto.
- Comunicación, con la suficiente antelación, a los usuarios afectados del momento de realización del cambio.
- Realización del cambio en horario de mínimo impacto.
- Documentación del cambio realizado y actualización de los documentos afectados por el cambio.

Procedimiento de actuación frente a un cambio de la política de seguridad

En este apartado se describe el procedimiento de actuación frente a la realización de un cambio en la política de seguridad de la red a llevar a cabo sobre un elemento de red de la infraestructura de seguridad perimetral.

Los pasos a seguir son los siguientes:

- Determinación del alcance del cambio, elementos afectados, implicaciones del cambio y duración del procedimiento de cambio (migración).
- Elaboración de un plan de cambio de red (o plan de migración).
- Autorización del cambio por parte de la organización.
- Programación del cambio en un horario acordado.
- Comunicación, con la suficiente antelación, a los usuarios afectados del momento de realización del cambio.
- Realización del cambio en el momento acordado.
- Documentación del cambio realizado y actualización de los documentos afectados por el cambio.

6. CONCLUSIONES

En este proyecto se ha tratado de dar a conocer lo que es la seguridad perimetral, primero sentando unas bases teóricas, para posteriormente exponer las fases necesarias para la implantación de un sistema de seguridad perimetral.

Para ello se ha partido de unos requisitos específicos, y una vez identificados, se ha ofrecido una solución que se adapte a dichos requisitos y cumpla en todo momento con un nivel de seguridad y un rendimiento óptimo. Además se han incluido unos métodos de gestión y mantenimiento de la plataforma una vez implantada.

En la definición de la arquitectura se ha optado por un modelo básico basado en dos niveles de cortafuegos. Actualmente este tipo de implementación garantiza un nivel de seguridad óptimo para las necesidades de la mayor parte de las organizaciones, pero no debemos caer en el error de delegar toda nuestra confianza en los cortafuegos como único elemento de seguridad. Un cortafuegos es un elemento fundamental en el diseño de cualquier topología básica, pero debe complementarse con otros componentes igualmente necesarios, como sondas de detección de intrusos, antivirus, gestores de ancho de banda, proxies, etc. La integración de todos ellos de forma adecuada complementa un sistema fiable y robusto, reduciendo considerablemente los riesgos y permitiendo detectar comportamientos anómalos que puedan afectar al rendimiento de nuestra red.

La situación actual en el campo de la seguridad perimetral ha evolucionado a un ritmo imparable en la última década. El número de amenazas ha crecido de manera exponencial y un entorno de seguridad perimetral se convierte en algo imprescindible actualmente.

El número de amenazas en los últimos años se ha disparado y el concepto de seguridad perimetral se ha convertido en una necesidad básica para cualquier organismo con acceso a Internet. Sin embargo esta evolución no ha hecho más que empezar y lo que ahora puede parecer un entorno seguro, dentro de unos años sin duda se habrá quedado obsoleto. El avance en las tecnologías trae consigo la aparición de nuevas amenazas y sin duda serán necesarios también nuevos sistemas de protección que minimicen los riesgos que vayan surgiendo.

La previsión de aquí a unos años en el campo de la seguridad perimetral es impredecible. El desarrollo de nuevos sistemas de seguridad es inevitable, y serán tan imprescindibles como los son actualmente los cortafuegos o antivirus. Será necesario adaptar nuestra infraestructura ya obsoleta a las nuevas tecnologías, bien ampliando los recursos existentes o sustituyéndolos por sistemas más avanzados.

En cualquier caso, el campo de la seguridad perimetral no ha hecho más que comenzar su andadura y será necesario adaptarse a los continuos cambios para no quedarnos atrás.

7. BIBLIOGRAFÍA

[1] *http://pics.unlugarenelmundo.es*

[2] *http://stuff.mit.edu*

[3] *http://www.securitybydefault.com*

[4] Desarrollo Web. Disponible en *http://www.desarrolloweb.com*

[5] Wikipedia. Disponible en *http://es.wikipedia.org*

[6] *http://www.configurarequipos.com*

[7] *http://www.articulosinformativos.com.mx*

[8] *http://www.ordenadores-y-portatiles.com*

[9] *http://www.n-experts.com*

[10] *http://doc.ubuntu-es.org*

[11] *http://www.esacademic.com*

[12] Allot Communications. Disponible en *http://www.allot.com*

[13] BlueCoat. Disponible en *http://www.bluecoat.com*

[14] StoneSoft. Disponible en *http://www.stonesoft.com*

[15] SafeNet. Disponible en *http://www.safenet-inc.es*

[16] HP. Fichas técnicas de servidores. Disponible en *http://www.hp.com*

[17] Optenet. Disponible en *http://www.optenet.es*

[18] IBM Internet Security Systems. Disponible en *http://www.iss.net*

[19] *http://www.liberaliatempus.com*

[20]Microsoft. Disponible en *http://www.microsoft.com*

[21] *http://www.linuxparatodos.net*

[22] *http://tuxjm.net*

[23] Microsoft. Disponible en *http://technet.microsoft.com*

[24] Check Point. Disponible en *http://www.checkpoint.com*

[25] *www.virtuality.es*

[26] SolarWinds. Disponible en *http://www.solarwinds.com*